Red Hat Certificate System 8.1 Agents Guide

Using Web-Based Agent Services
Edition 1

Ella Deon Ballard

Red Hat Certificate System 8.1 Agents Guide

Using Web-Based Agent Services
Edition 1

Ella Deon Ballard
dlackey@redhat.com

Legal Notice

Copyright © 2012 Red Hat, Inc.

This document is licensed by Red Hat under the Creative Commons Attribution-ShareAlike 3.0 Unported License. If you distribute this document, or a modified version of it, you must provide attribution to Red Hat, Inc. and provide a link to the original. If the document is modified, all Red Hat trademarks must be removed.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, MetaMatrix, Fedora, the Infinity Logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat Software Collections is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack Logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Abstract

for agents to manage certificate requests and other operations

Table of Contents

About This Guide **5**
1. Required Concepts 5
2. What Is in This Guide 5
3. Examples and Formatting 6
3.1. Formatting for Examples and Commands 6
3.2. Tool Locations 6
3.3. Guide Formatting 6
4. Additional Reading 7
5. Giving Feedback 8
6. Document History 8

Chapter 1. Agent Services **9**
1.1. Overview of Certificate System 9
1.1.1. Certificate System Subsystems 9
1.1.1.1. Certificate Manager 9
1.1.1.2. Registration Manager 9
1.1.1.3. Data Recovery Manager 10
1.1.1.4. Online Certificate Status Manager 10
1.1.1.5. Token Processing System 10
1.1.2. Certificate System Users 10
1.2. Agent Tasks 11
1.2.1. Certificate Manager Agent Services 12
1.2.2. Registration Manager Agent Services 13
1.2.3. Data Recovery Manager Agent Services 14
1.2.4. Online Certificate Status Manager Agent Services 15
1.2.5. Token Processing System Agent Services 16
1.3. Accessing Agent Services 18
1.4. Using and Recovering Agent Certificates 19
1.5. Using Java Servlets with Subsystem Web Forms 20
1.6. Supported Web Browsers 20
1.7. Supported Character Sets 20
1.8. Configuring Internet Explorer to Enroll Certificates 21

Chapter 2. CA: Working with Certificate Profiles **23**
2.1. About Certificate Profiles 23
2.2. Example caUserCert Profile 24
2.3. List of Certificate Profiles 27
2.4. Enabling and Disabling Certificate Profiles 30
2.4.1. Viewing Certificate Profile Information 31
2.4.2. Enabling or Disabling a Certificate Profile 33

Chapter 3. CA: Handling Certificate Requests **34**
3.1. Managing Requests 34
3.2. Listing Certificate Requests 36
3.2.1. Selecting a Request 38
3.2.2. Searching for Certificates (Advanced) 39
3.3. Approving Requests 45
3.4. Sending an Issued Certificate to the Requester 47

Chapter 4. CA: Finding and Revoking Certificates **50**
4.1. Listing Certificates 50
4.2. Searching for Certificates (Advanced) 51
4.3. Examining Certificate Details 54

4.4. Revoking Certificates 55
4.4.1. Revoking Certificates 55
4.4.2. Taking Ceritificates Off Hold 58
4.5. Managing the Certificate Revocation List 59
4.5.1. Viewing or Examining CRLs 59
4.5.2. Updating the CRL 60

Chapter 5. CA: Publishing to a Directory 62
5.1. Automatically Updating the Directory 62
5.2. Manually Updating the Directory 62

Chapter 6. RA: Requesting and Receiving Certificates Locally 65
6.1. Listing Certificate Requests 65
6.2. Approving Certificate Requests 67
6.3. Listing Certificates 68
6.4. Revoking Certificates 70
6.5. Creating and Managing Users and Groups for an RA 71
6.5.1. Managing RA Groups 72
6.5.1.1. Listing Groups for an RA 72
6.5.1.2. Creating a New Group for an RA 72
6.5.1.3. Adding and Removing Users in an RA Group 73
6.5.2. Managing RA Users 74
6.5.2.1. Listing and Viewing Users for an RA 75
6.5.2.2. Creating a New User for an RA 76
6.5.2.3. Generating Agent Certificates for RA Agents 77

Chapter 7. DRM: Recovering Encrypted Data 81
7.1. Listing Requests 81
7.2. Finding Archived Keys 83
7.3. Recovering Keys 86
7.3.1. Recovering Keys: Asynchronous Recovery 88
7.3.1.1. Initiating Key Recovery 88
7.3.1.2. Getting Agent Approval for Key Recovery 90
7.3.1.3. Recovering the Key 90
7.3.2. Recovering Keys: Synchronous Recovery 91
7.3.2.1. Initiating Key Recovery 91
7.3.2.2. Getting Agent Approval for Key Recovery 93
7.3.2.3. Recovering the Key 94

Chapter 8. Online Certificate Status Manager: Verifying Certificate Status 96
8.1. Listing CAs Identified by the Online Certificate Status Manager 96
8.2. Identifying a CA to the Online Certificate Status Manager 97
8.3. Removing a CA from the OCSP Manager 99
8.4. Adding a CRL to the Online Certificate Status Manager 99
8.5. Checking the Revocation Status of a Certificate 101
8.6. OCSP Responder Summary 103

Chapter 9. TPS: Managing Token and Smart Card Operations 105
9.1. Overview of TPS Roles 105
9.2. Performing Operator Tasks 106
9.2.1. Searching Tokens 107
9.2.2. Viewing Tokens 108
9.2.3. Searching Certificates 109
9.2.4. Searching Activities 110
9.3. Performing Agent Tasks 111
9.3.1. Searching Tokens 112

9.3.2. Viewing Tokens 113
9.3.3. Managing Tokens 114
9.3.3.1. Editing the Token Information 114
9.3.3.2. Changing the Token Policy 115
9.3.3.3. Changing Token Status 116
9.3.4. Searching Certificates 119
9.3.5. Searching Activities 120
9.3.6. Enabling and Disabling Profiles 121
9.3.6.1. Enabling Profiles 121
9.3.6.2. Disabling Profiles 122
9.4. Performing Administrator Tasks 123
9.4.1. Managing Tokens 124
9.4.1.1. Adding Tokens 125
9.4.1.2. Searching Tokens 125
9.4.1.3. Viewing Tokens 125
9.4.1.4. Deleting the Token 126
9.4.2. Managing TPS Users 127
9.4.2.1. Searching Users 127
9.4.2.2. Adding Users 127
9.4.2.3. Setting Profiles for Users 128
9.4.2.4. Changing Roles for Users 129
9.4.2.5. Deleting Users 129
9.4.3. Searching Activities 130
9.4.4. Running Self-Tests 131
9.4.5. Managing the TPS Audit Logs 131
9.4.6. Managing TPS Server Configuration 134
9.4.6.1. Editing TPS Profiles 135
9.4.6.2. Mapping Token Types and TPS Policies 136
9.4.6.3. Configuring Connections to Other Subsystems 139
9.4.6.4. Editing LDAP Authentication Sources 140
9.4.6.5. Setting TPS Server General Configuration 142
9.5. Conflicting Token Certificate Status Information 143

Index **144**
A 144
C 144
D 145
E 146
F 146
I 146
L 146
M 146
N 146
O 146
P 146
R 147
S 147
T 147

About This Guide

The web-based interfaces for Certificate System allow end users, agents, and administrators to perform common tasks, such as requesting, approving, and revoking certificates. Additionally, administrators for RA and TPS subsystems can perform administrative tasks such as creating users and groups. This guide is for agents of Certificate System subsystems. It explains the different agent services interfaces for the Certificate System subsystems and details the agent operations which can be performed. This information is used to manage and maintain certificates and keys for users in the PKI deployment.

This guide is intended for Certificate System agents. Agents are privileged users designated by the Certificate System administrator to manage requests from end entities for certificate-related services. Each installed Certificate System subsystem; Certificate Manager, Data Recovery Manager (DRM), Online Certificate Status Manager, Token Key Service (TKS), and Token Processing System (TPS), can have multiple agents.

1. Required Concepts

Before reading this guide, be familiar with the basic concepts of public-key cryptography and the Secure Sockets Layer (SSL) protocol, including the following topics:

- Encryption and decryption
- Public keys, private keys, and symmetric keys
- Digital signatures
- The role of digital certificates in a public-key infrastructure (PKI)
- Certificate hierarchies
- SSL cipher suites
- The purpose of and major steps in the SSL handshake

2. What Is in This Guide

This guide describes an agent's responsibilities for the different Certificate System subsystems, and explains basic usage and tasks.

- Chapter 1, *Agent Services* Provides an overview of the product and identifies different kinds of users, including agents. The chapter also summarizes the tasks of each subsystem agent, lists the HTML forms used to perform agent tasks, and explains how to access the agent services pages and forms.
- Chapter 2, *CA: Working with Certificate Profiles* Provides an overview of the profiles feature and details how to enable and disable profiles.
- Chapter 3, *CA: Handling Certificate Requests* Describes the general procedures for handling requests and explains how to handle different aspects of certificate request management. A Certificate Manager agent is responsible for handling requests by end entities (end users, server administrators, or other Certificate System subsystems) for certificates using manual enrollment.
- Chapter 4, *CA: Finding and Revoking Certificates* Explains how to use the agent services page to find and examine a specific certificate issued by Certificate System, how to retrieve a list of certificates that match specified criteria, how to revoke certificates, and how to manage the certificate revocation list.
- Chapter 5, *CA: Publishing to a Directory* Describes how a Certificate Manager agent can update the LDAP directory with the current status of certificates.
- Chapter 7, *DRM: Recovering Encrypted Data* Describes how to process key recovery requests and how to recover stored encrypted data when the encryption key has been lost. This service is only available when a Data Recovery Manager (DRM) is installed.

- Chapter 8, *Online Certificate Status Manager: Verifying Certificate Status* Describes how to handle tasks related to the Certificate System OCSP responder, Online Certificate Status Manager. This service is only available when the OCSP subsystem is installed.
- Chapter 9, *TPS: Managing Token and Smart Card Operations* Describes how to perform tasks related to the Token Processing System and how to manage tokens and certificates through this subsystem. This service is only available when the TPS subsystem is installed.

3. Examples and Formatting

3.1. Formatting for Examples and Commands

All of the examples for Red Hat Certificate System commands, file locations, and other usage are given for Red Hat Enterprise Linux 5.6 (32-bit) systems. Be certain to use the appropriate commands and files for your platform.

> **Example 1. Example Command**
>
> To start the Red Hat Certificate System:
>
> ```
> service pki-ca start
> ```

3.2. Tool Locations

All of the tools for Red Hat Certificate System are located in the **/usr/bin** directory. These tools can be run from any location without specifying the tool location.

3.3. Guide Formatting

Certain words are represented in different fonts, styles, and weights. Different character formatting is used to indicate the function or purpose of the phrase being highlighted.

Formatting Style	Purpose
Monospace font	Monospace is used for commands, package names, files and directory paths, and any text displayed in a prompt.
`Monospace with a background`	This type of formatting is used for anything entered or returned in a command prompt.
Italicized text	Any text which is italicized is a variable, such as *instance_name* or *hostname*. Occasionally, this is also used to emphasize a new term or other phrase.
Bolded text	Most phrases which are in bold are application names, such as **Cygwin**, or are fields or options in a user interface, such as a **User Name Here:** field or **Save** button.

Other formatting styles draw attention to important text.

NOTE

A note provides additional information that can help illustrate the behavior of the system or provide more detail for a specific issue.

IMPORTANT

Important information is necessary, but possibly unexpected, such as a configuration change that will not persist after a reboot.

WARNING

A warning indicates potential data loss, as may happen when tuning hardware for maximum performance.

4. Additional Reading

The documentation for Certificate System includes the following guides:

- *Certificate System Deployment Guide* describes basic PKI concepts and gives an overview of the planning process for setting up Certificate System.

  This manual is intended for Certificate System administrators.
- *Certificate System Installation Guide* covers the installation process for all Certificate System subsystems.

  This manual is intended for Certificate System administrators.
- *Certificate System Administrator's Guide* explains all administrative functions for the Certificate System. Administrators maintain the subsystems themselves, so this manual details backend configuration for certificate profiles, publishing, and issuing certificates and CRLs. It also covers managing subsystem settings like port numbers, users, and subsystem certificates.

  This manual is intended for Certificate System administrators.
- *Certificate System Agent's Guide* describes how agents — users responsible for processing certificate requests and managing other aspects of certificate management — can use the Certificate System subsystems web services pages to process certificate requests, key recovery, OCSP requests and CRLs, and other functions.

  This manual is intended for Certificate System agents.
- *Managing Smart Cards with the Enterprise Security Client* explains how to install, configure, and use the Enterprise Security Client, the user client application for managing smart cards, user certificates, and user keys.

  This manual is intended for Certificate System administrators, agents, privileged users (such as security officers), and regular end users.
- *Using End User Services* is a quick overview of the end-user services in Certificate System, a simple way for users to learn how to access Certificate System services.

  This manual is intended for regular end users.
- *Certificate System Command-Line Tools Guide* covers the command-line scripts supplied with Red Hat Certificate System.

This manual is intended for Certificate System administrators.

- *Certificate System Migration Guide* covers version-specific procedures for migrating from older versions of Certificate System to Red Hat Certificate System 8.1.

  This manual is intended for Certificate System administrators.

- *Release Notes* contains important information on new features, fixed bugs, known issues and workarounds, and other important deployment information for Red Hat Certificate System 8.1.

All of the latest information about Red Hat Certificate System and both current and archived documentation is available at http://www.redhat.com/docs/manuals/cert-system/.

5. Giving Feedback

If there is any error in this *Agent's Guide* or there is any way to improve the documentation, please let us know. Bugs can be filed against the documentation for Red Hat Certificate System through Bugzilla, http://bugzilla.redhat.com/bugzilla. Make the bug report as specific as possible, so we can be more effective in correcting any issues:

- Select the Red Hat Certificate System product.
- Set the component to **`Doc - agents-guide`**.
- Set the version number to 8.1.
- For errors, give the page number (for the PDF) or URL (for the HTML), and give a succinct description of the problem, such as incorrect procedure or typo.

  For enhancements, put in what information needs to be added and why.
- Give a clear title for the bug. For example, **`"Incorrect command example for setup script options"`** is better than **`"Bad example"`**.

We appreciate receiving any feedback — requests for new sections, corrections, improvements, enhancements, even new ways of delivering the documentation or new styles of docs. You are welcome to contact Red Hat Content Services directly at docs@redhat.com.

6. Document History

Revision 8.1-4	**June 27, 2011**	**Ella Deon Lackey**

Added new audit events, from Bugzilla #707416.

Revision 8.1-0	**June 1, 2011**	**Ella Deon Lackey**

Initial draft for Certificate System 8.1 documentation.

Chapter 1. Agent Services

This chapter describes the role of the privileged users, *agents*, in managing Certificate System subsystems. It also introduces the tools that agents use to administer service requests.

1.1. Overview of Certificate System

The Red Hat Certificate System is a highly configurable set of software components and tools for creating, deploying, and managing certificates. The standards and services that facilitate the use of public-key cryptography and X.509 version 3 certificates in a networked environment are collectively called the *public-key infrastructure* (PKI) for that environment. In any PKI, a *certificate authority* (CA) is a trusted entity that issues, renews, and revokes certificates. An *end entity* is a person, server, or other entity that uses a certificate to identify itself.

To participate in a PKI, an end entity must *enroll*, or register, in the system. The end entity typically initiates enrollment by giving the CA some form of identification and a newly generated public key. The CA uses the information provided to *authenticate*, or confirm, the identity, then issues the end entity a certificate that associates that identity with the public key and signs the certificate with the CA's own private signing key.

End entities and CAs can exist in different geographic or organizational areas or in completely different organizations. CAs may include third parties that provide services through the Internet as well as the root CAs and subordinate CAs for individual organizations. Policies and certificate content may vary from one organization to another. End-entity enrollment for some certificates may require physical verification, such as an interview or notarized documents, while enrollment for others may be fully automated.

1.1.1. Certificate System Subsystems

To meet the widest possible range of configuration requirements, the Certificate System permits independent installation of five separate subsystems, or *managers*, that play distinct roles.

1.1.1.1. Certificate Manager

A Certificate Manager functions as a root or subordinate certificate authority (CA). This subsystem issues, renews, and revokes certificates and generates certificate revocation lists (CRLs). It can also publish certificates, files, and CRLs to an LDAP directory, to files, and to an online certificate status protocol (OCSP) responder.

The Certificate Manager can process requests manually (with agent action) or automatically (based on customizable profiles). Publishing tasks can only be performed by the Certificate Manager.

The Certificate Manager also has a built-in OCSP service, enabling OCSP-compliant clients to query the Certificate Manager directly about the revocation status of a certificate that it has issued. In certain PKI deployments, it might be convenient to use the Certificate Manager's built-in OCSP service, instead of a separate Online Certificate Status Manager.

Because CAs can delegate some responsibilities to subordinate CAs, a Certificate Manager might share its load among one or more levels of subordinate Certificate Managers.

Subsystems can also be cloned. All clones use the same keys and certificates as the master, which means that the master and clones essentially all function as a single CA. Many complex deployment scenarios are possible.

1.1.1.2. Registration Manager

A registration authority is an intermediary between a user or location and a CA. The registration

authority processes and authenticates enrollment requests; approved requests are then sent to the CA for it to issue the new certificate. Breaking the approval and issuance steps into separate subsystems takes some of the burden off centralized CAs.

RAs agents can approve or reject certificate requests. They can also revoke certificates which they approved.

1.1.1.3. Data Recovery Manager

A Data Recovery Manager (DRM) oversees the long-term archival and recovery of private encryption keys for end entities. A Certificate Manager or TPS can be configured to archive end entities' private encryption keys with a DRM as part of the process of issuing new certificates.

The DRM is useful only if end entities are encrypting data, using applications such as S/MIME email, that the organization may need to recover someday. It can be used only with client software that supports dual key pairs; two separate key pairs, one for encryption and one for digital signatures. It is also possible to perform server-side key generation using the TPS server when enrolling smart cards.

NOTE

The DRM archives encryption keys. It does not archive signing keys, since archiving signing keys would undermine the non-repudiation properties of dual-key certificates.

1.1.1.4. Online Certificate Status Manager

An Online Certificate Status Manager works as an online certificate validation authority and allows OCSP-compliant clients to verify certificates' current status. The Online Certificate Status Manager can receive CRLs from multiple Certificate Managers; clients then query the OCSP service for the revocation status of certificates issued by all Certificate Managers. For example, in a PKI comprising multiple CAs (a root CA and many subordinate CAs), each CA can be configured to publish its CRL to the Online Certificate Status Manager, allowing all clients in the PKI deployment to verify the revocation status of a certificate by querying a single OCSP service.

NOTE

An online certificate-validation authority is often referred to as an *OCSP responder*.

1.1.1.5. Token Processing System

The Token Processing System (TPS) acts as a registration authority for authenticating and processing smart card enrollment requests, PIN reset requests, and formatting requests from the Enterprise Security Client.

1.1.2. Certificate System Users

Three kinds of users can access Certificate System subsystems: administrators, agents, and end entities. Administrators are responsible for the initial setup and ongoing maintenance of the subsystems. Administrators can also assign *agent* status to users. Agents manage day-to-day interactions with end entities, which can be users or servers and clients, and other aspects of the PKI. End entities must access a Certificate Manager (CA) subsystem to enroll for certificates in a PKI deployment and for certificate maintenance, such as renewal or revocation.

Figure 1.1, “The Certificate System and Users” shows the ports used by administrators, agents, and end

entities. All agent and administrator interactions with Certificate System subsystems occur over HTTPS. End-entity interactions can take place over HTTP or HTTPS.

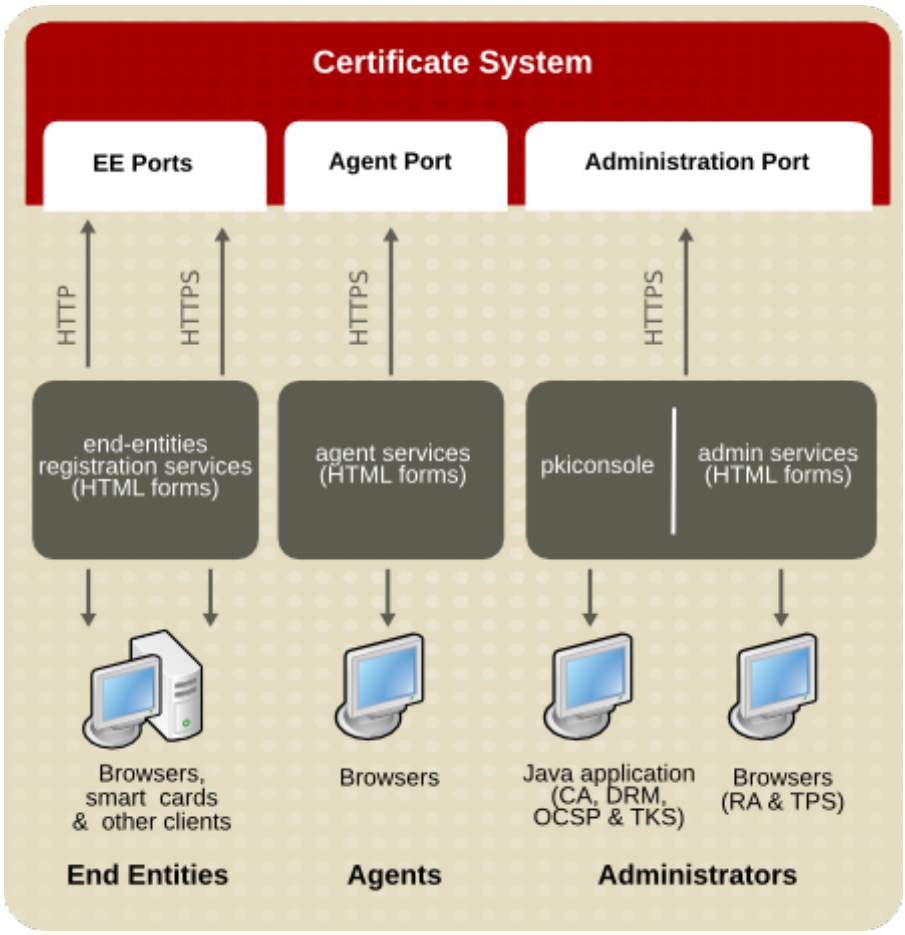


Figure 1.1. The Certificate System and Users

1.2. Agent Tasks

The designated agents for each subsystem are responsible for the everyday management of end entity requests and other aspects of the PKI:

- *Certificate Manager Agents* manage certificate requests received by the Certificate Manager subsystem, maintain and revoke certificates as necessary, and maintain global information about certificates.
- *Registration Manager Agents* process certificate requests; any approved requests are automatically forwarded to the configured CA to issue the certificate. RA agents can also revoke certificates which have been issued through the RA.
- *Data Recovery Manager Agents* initiate the recovery of lost keys and can obtain information about key service requests and archived keys.

NOTE

Recovering lost or archived key information is done automatically in smart card deployments because the TPS server is a DRM agent. Smart cards are marked as lost in the TPS agent page, and then another smart card is later used to recover the old encryption keys automatically during certificate enrollment.

- *Online Certificate Status Manager Agents* manage the configuration for verifying whether certificates are revoked, so these agents can both manage CRLs (by managing the publishing CAs and manually adding CRLs) and manage requests to check certificate status.
- *Token Processing System Agents* can perform tasks related to managing certificates stored on tokens and smart cards, which includes viewing smart card enrollment and formatting activities; listing, editing, and deleting tokens from the token database; and managing lost tokens.

The privileged operations of an agent are performed through the Certificate System agent services pages. For a user to access these pages, the user must have a personal SSL client certificate and have been identified as a privileged user in the user database by the Certificate System administrator. For more information on creating privileged users, see the *Certificate System Administrator's Guide*.

- Section 1.2.1, “Certificate Manager Agent Services”
- Section 1.2.2, “Registration Manager Agent Services”
- Section 1.2.3, “Data Recovery Manager Agent Services”
- Section 1.2.4, “Online Certificate Status Manager Agent Services”
- Section 1.2.5, “Token Processing System Agent Services”

1.2.1. Certificate Manager Agent Services

The default entry page for CA agent services is shown in Figure 1.2, “Certificate Manager Agent Services Page”. Only designated Certificate Manager agents, with a valid certificate installed in their client software, are authorized to access these pages.

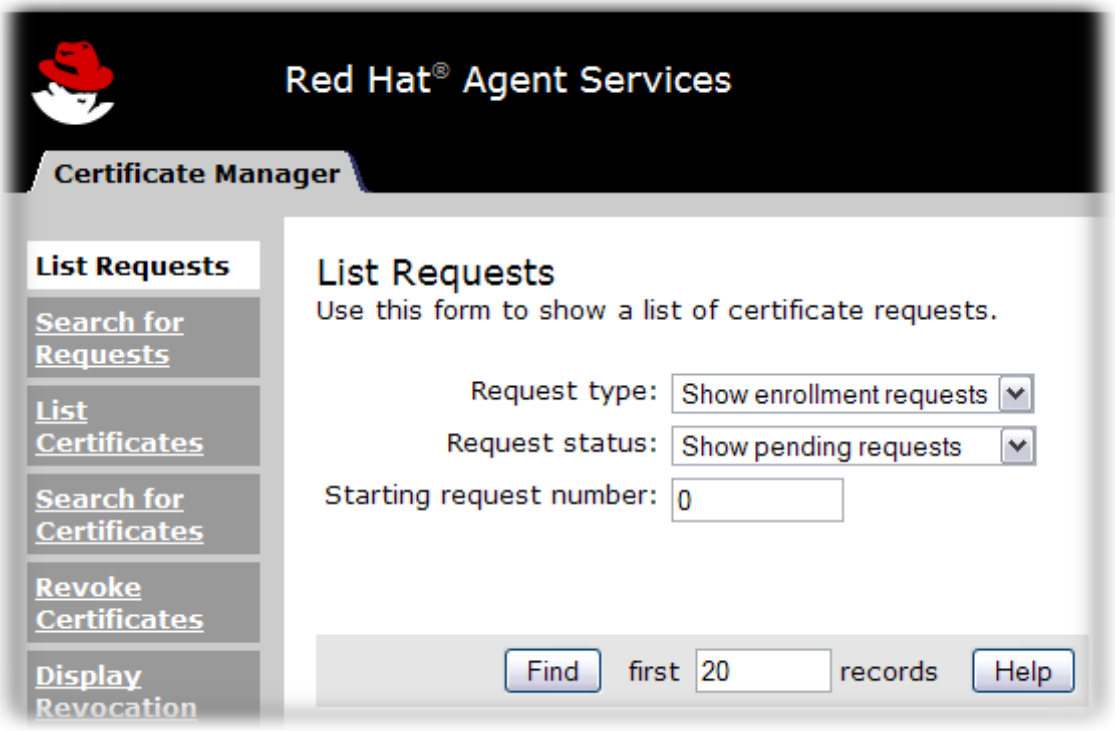


Figure 1.2. Certificate Manager Agent Services Page

A Certificate Manager agent performs the following tasks:

- Handles certificate requests.

  An agent can list the certificate service requests received by the Certificate Manager subsystem, assign requests, reject or cancel requests, and approve requests for certificate enrollment. See Chapter 3, *CA: Handling Certificate Requests*.
- Finds certificates.

  Certificates can be searched for individually or searched and listed by different criteria. The details for all returned certificates are then displayed. See Chapter 4, *CA: Finding and Revoking Certificates*.
- Revokes certificates.

  If a user's key is compromised, the certificate must be revoked to ensure that the key is not misused. Certificates belonging to users who have left the organization may also need revoked. Certificate Manager agents can find and revoke a specific certificate or a set of certificates. Users can also request that their own certificates be revoked. See Section 4.4, “Revoking Certificates”.
- Updates the CRL.

  The Certificate Manager maintains a public list of revoked certificates, called the Certificate Revocation List (CRL). The list is usually maintained automatically, but, when necessary, the Certificate Manager agent services page can be used to update the list manually. See Section 4.5.2, “Updating the CRL”.
- Publishes certificates to a directory.

  The Certificate System can be configured to publish certificates and CRLs to an LDAP directory. This information is usually published automatically, but the Certificate Manager agent services page can be used to update the directory manually. See Section 5.2, “Manually Updating the Directory”.
- Manages certificate profiles.

  The agent can enable and disable certificate profiles. A profile must be temporarily disabled before an administrator can make changes to the profile itself using the administrative interface. After the changes have been made, the agent can re-enable the profile for regular use. See Chapter 2, *CA: Working with Certificate Profiles*.

1.2.2. Registration Manager Agent Services

There are two user types who can access the RA services pages: agents and administrators. Each user requires a certificate to authenticate to the appropriate services page.

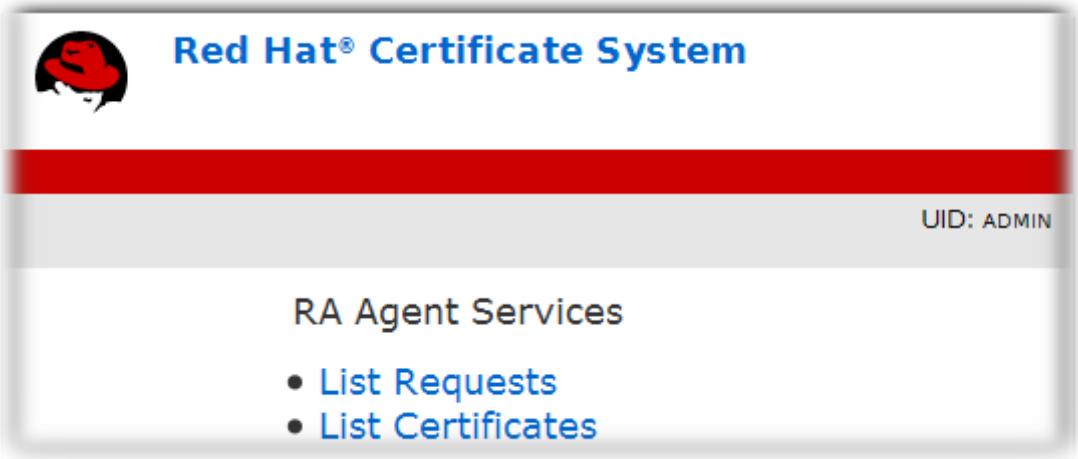


Figure 1.3. Registration Manager Agent Services Page

RA agents can perform four tasks:

- Approve and reject certificate requests.
- List, view, and add notes to certificate requests.
- List and view issued certificates.
- Revoke issued certificates.

RA agents cannot *initiate* tasks, in a sense. Their services page begins with listing requests and certificates because the agent's job is to respond to enrollment operations initiated by users.

RA administrators can only manage users and groups for the RA subsystem.

NOTE

The RA subsystem uses its HTML-based services pages for administrative functions as well as agent services, because it does not have a Java-based console to handle those administrative tasks. For the RA, those administrative tasks relate to managing users and groups.

1.2.3. Data Recovery Manager Agent Services

Only designated DRM agents, with a valid certificate installed in their browser, are authorized to access the agent services pages.

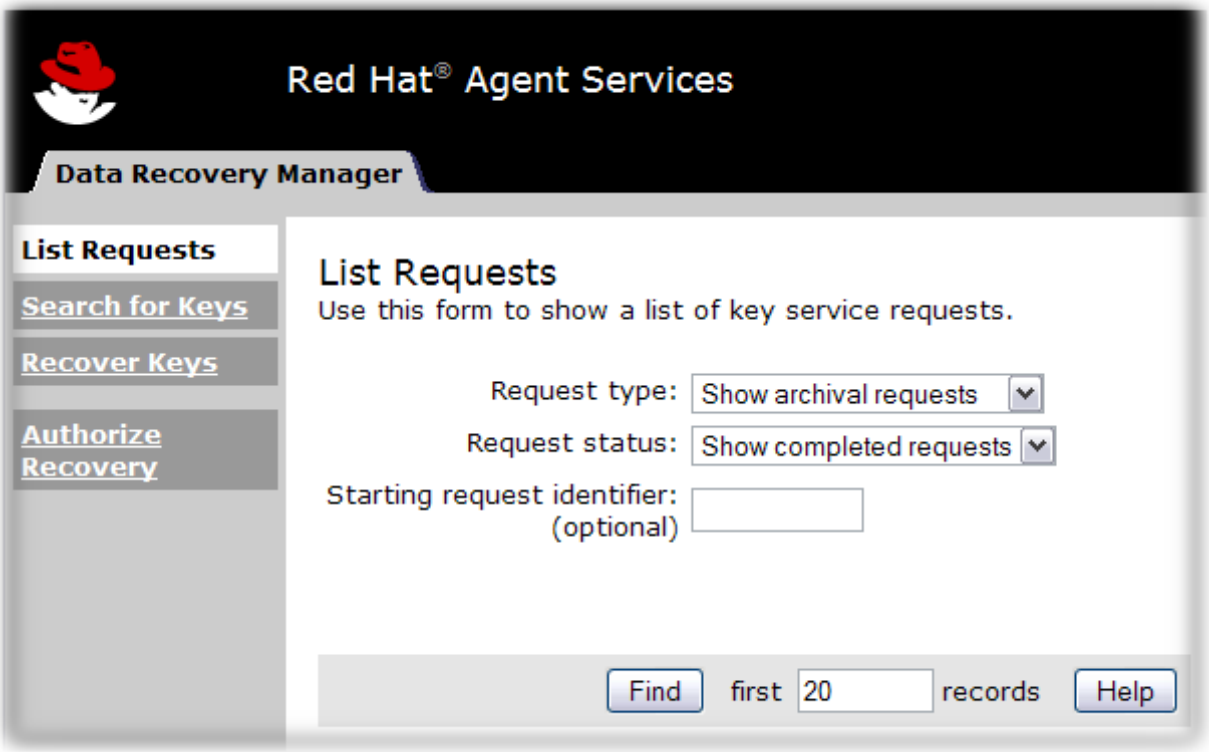


Figure 1.4. Data Recovery Manager Agent Services Page

A DRM agent performs the following tasks:

- Lists key recovery requests from end entities.
- Lists or searches for archived keys.
- Recovers private data-encryption keys.
- Authorizes and approves key recovery requests.

  Key recovery requires the authorization of one or more *recovery agents*. The DRM administrator designates recovery agents. Typically, several recovery agents are required to approve key recovery requests in the DRM, so DRM administrators should designate more than one agent.

For more information on these tasks, see Chapter 7, *DRM: Recovering Encrypted Data*.

1.2.4. Online Certificate Status Manager Agent Services

The default entry page to the Online Certificate Status Manager agent services is shown in Figure 1.5, "Online Certificate Status Manager Agent Services Page". Only designated Online Certificate Status Manager agents, with a valid certificate in their client software, are authorized to access these pages.

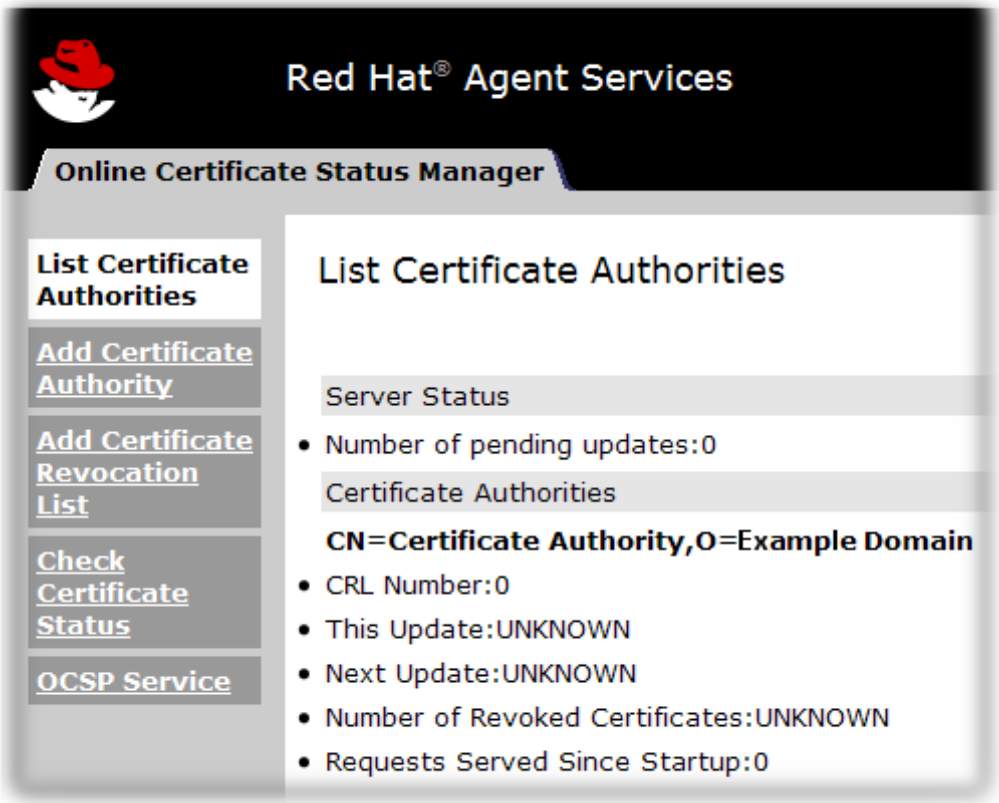


Figure 1.5. Online Certificate Status Manager Agent Services Page

An Online Certificate Status Manager agent performs the following tasks:

- Checks that CAs are currently configured to publish their CRLs to the Online Certificate Status Manager.
- Identifies a Certificate Manager to the Online Certificate Status Manager.
- Manually adds CRLs to the Online Certificate Status Manager.
- Submits requests for the revocation status of a certificate to the Online Certificate Status Manager.

For more information on these tasks, see Chapter 8, *Online Certificate Status Manager: Verifying Certificate Status*.

1.2.5. Token Processing System Agent Services

The TPS agent services page allows operations by two types of users, both agents and administrators. A third user type, operators, can view certificate and token information, but cannot edit or process token information.

The default entry page to the Token Processing System (TPS) agent services is shown in Figure 1.6, "TPS Agent Services Page". Only designated TPS agents, with a valid certificate in their client software, are authorized to access these pages.

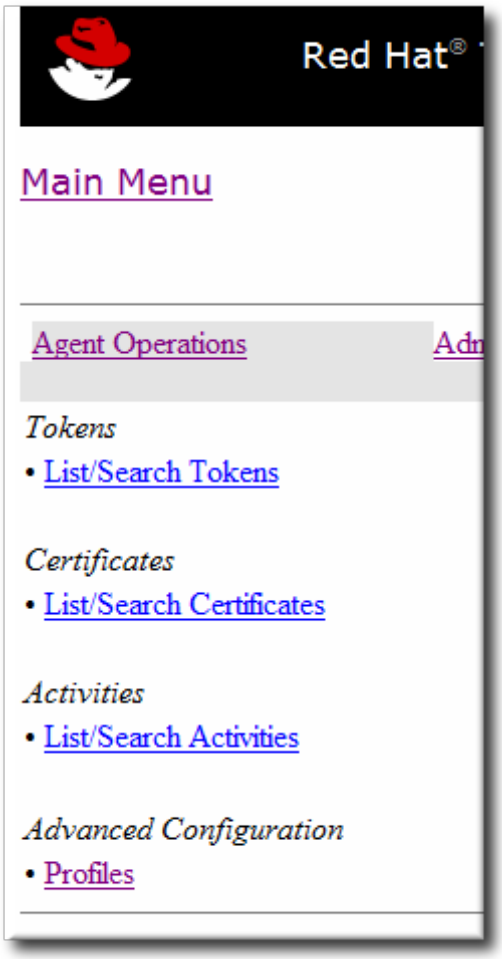


Figure 1.6. TPS Agent Services Page

A TPS agent performs the following tasks:

- Lists and searches enrolled tokens by user ID or token CUID.
- Lists and searches certificates associated with enrolled tokens.
- Searches token operations by CUID.
- Edits token information.
- Sets the token status.

The TPS agent services page also has a tab to allow operations by TPS administrators.

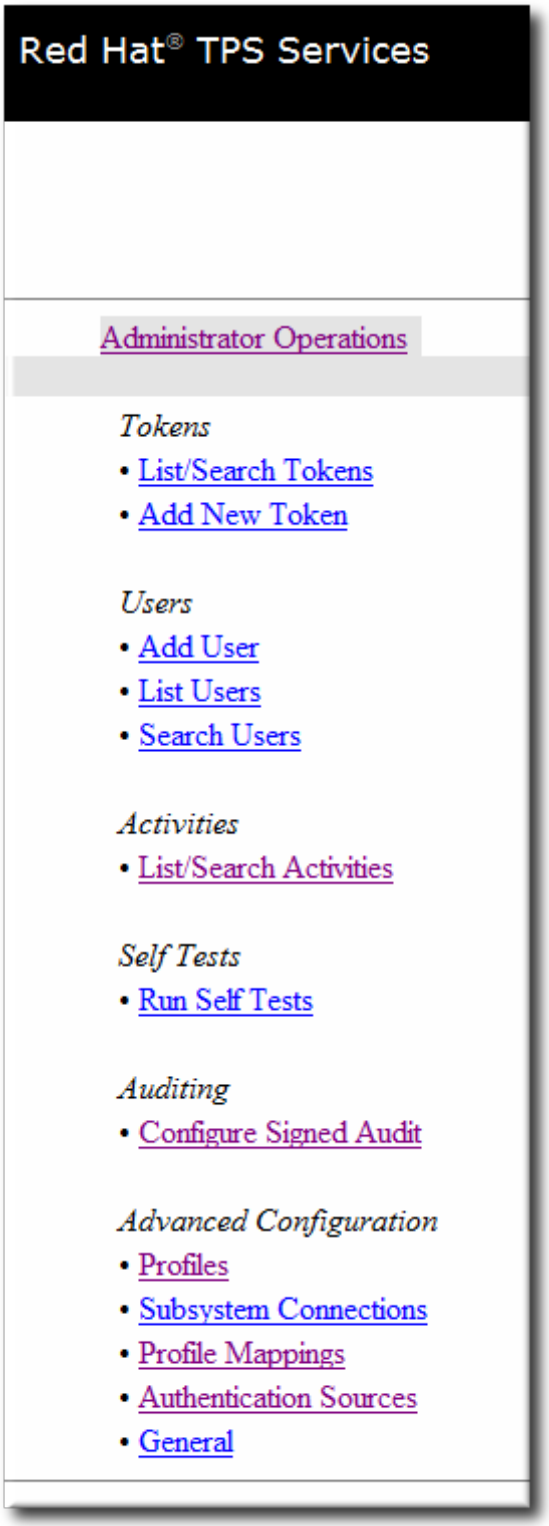


Figure 1.7. TPS Administrator Operations Tab

A TPS administrator performs the following tasks:

- Lists and searches enrolled tokens by user ID or token CUID.
- Edits token information, including the token owner's user ID.
- Adds tokens.
- Deletes tokens.

For more information about TPS agent and administrator tasks, see Chapter 9, *TPS: Managing Token and Smart Card Operations*.

1.3. Accessing Agent Services

Access to the agent services forms requires certificate-based authentication. Only users who authenticate with the correct certificate and who have been granted the appropriate access privilege can access and use the forms. Operations are performed over SSL, so the server connection uses HTTPS on the SSL agent port.

The agent services URLs use the following format:

```
https://hostname:port/subsystem_type/agent/subsystem_type
```

The *hostname* can be a fully-qualified domain name, simply the hostname (if it is on an intranet), or an IPv4 or IPv6 address.

The *port* is the SSL port number used to access agent services (there are two other SSL ports for administrative and end user services, as well). The default agent SSL port numbers for the subsystem are as follows:

- 9443 for the CA
- 10443 for the DRM
- 12889 for the RA
- 11443 for the OCSP
- 7889 for the TPS

The port number may be different if the agent services use a user-defined port set with the **-agent_secure_port** when the instance was created with **pkicreate**.

The *subsystem_type* type is one of the following:

- **ca** for the CA
- **ra** for the RA
- **kra** for the DRM
- **ocsp** for the Online Certificate Status Manager
- **tps** for the TPS

For example, if a CA is installed on a host named **server.example.com** and is listening on port 9443, the URL to access the agent services interface is **https://server.example.com:9443/ca/agent/ca**.

There is also a general services page for each subsystem. The services page has links to the all of the HTML pages for the subsystem, such as agent and end entities, as well as the administration page if the subsystem has not yet been configured. The URL for the services page, for this example, is **https://server.example.com:9445/ca/services**.

Red Hat Certificate System
Certifcate System
Certificate System Services Page
SSL End Users Services
Agent Services
Copyright © 2002-06 Red Hat, Inc. All rights reserved. http://www.redhat.com

Figure 1.8. Certificate Manager Services Page

NOTE

The services pages are written in HTML and are intended to be customized. This document describes the default pages. If an administrator has customized the agent services pages, those pages may differ from those described here. Check with the Certificate System administrator for information on the local installation.

1.4. Using and Recovering Agent Certificates

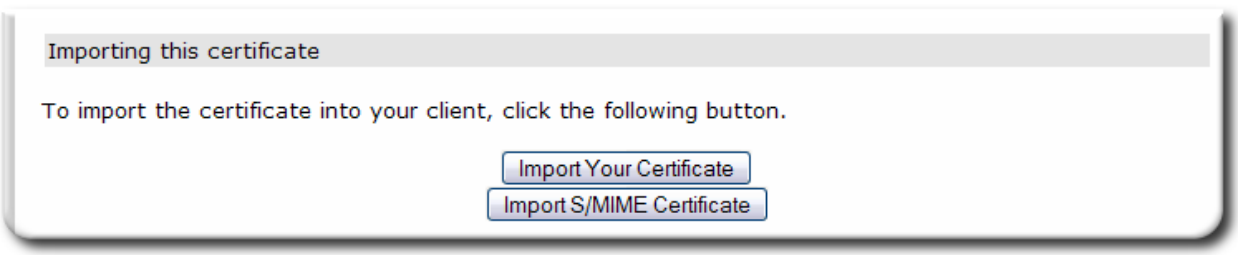
As mentioned in Section 1.3, “Accessing Agent Services”, agents use certificates to authenticate to the agent services pages. These certificates are imported into the browser user to access the agent (and administrative, for the TPS and RA) services pages.

The agent certificate can be imported into a new browser or recovered and re-imported into a browser if it is ever lost. Retrieve the agent or user certificates from the CA's end entities page, and import them into the browser to use for accessing the agent services pages.

1. Open the CA's end entities pages.

   ```
   https://server.example.com:9444/ca/ee/ca
   ```

2. In the **Retrieval** tab, search for the agent's certificates in the list of issued certificates.
3. Select the agent certificate from the list.
4. Scroll to the bottom of the certificate's page, and click the **Import ... Certificate** button.


Importing this certificate
To import the certificate into your client, click the following button.
Import Your Certificate
Import S/MIME Certificate

1.5. Using Java Servlets with Subsystem Web Forms

Each subsystem Java™ servlet supports a parameter called **xml**, which can have a value of either **true** or **false**. This parameter sets what kind of data the servlet returns; by default all of the subsystem interfaces, like the agent services page or the end-entities page, returns data in HTML.

Setting the **xml** with a value of **true** returns XML data. This XML information is useful for writing scripts that interact with the server.

The **xml** parameter is appended to the end of the interface link. For example, the server returns an HTML page when the following link is accessed:

```
https://server.example.com:9444/ca/ee/ca/displayBySerial?
op=displayBySerial&serialNumber=0x1
```

Appending **xml=true** to the end of the link returns the same page in XML:

```
https://server.example.com:9444/ca/ee/ca/displayBySerial?
op=displayBySerial&serialNumber=0x1&xml=true
```

1.6. Supported Web Browsers

The services pages for the subsystems require a web browser that supports SSL. Two browsers are supported:

- Mozilla Firefox 2.0 and higher
- Microsoft Internet Explorer 6 and higher on both Windows XP and Vista

Red Hat strongly recommends that agents and administrators use Mozilla Firefox to access the agent services pages.

NOTE

Browsers for Mac, such as Safari, and other types of web browsers, such as Opera, are not supported for the agent services pages. This means that some operations may not complete successfully or forms may not be displayed properly.

1.7. Supported Character Sets

Red Hat Certificate System fully supports UTF-8 characters in the CA end users forms for specific fields. This means that end users can submit certificate requests with UTF-8 characters in those fields and can search for and retrieve certificates and CRLs in the CA and retrieve keys in the DRM when using those field values as the search parameters.

Four fields fully-support UTF-8 characters:

- Common name (used in the subject name of the certificate)
- Organizational unit (used in the subject name of the certificate)
- Requester name
- Additional notes (comments appended by the agent to the certificate)

NOTE

This support does not include supporting internationalized domain names.

1.8. Configuring Internet Explorer to Enroll Certificates

Because of the security settings in Microsoft Windows Vista, requesting and enrolling certificates through the end entities pages using Internet Explorer 7 and 8 requires extra browser configuration. The browser has to be configured to trust the CA before it can access the CA's secure end entities pages.

NOTE

This configuration is not necessary to use Internet Explorer 7 and 8 on Microsoft Windows 2000, 2003, or XP.

1. Open Internet Explorer.
2. Import the CA certificate chain.
    a. Open the unsecure end services page for the CA.

    ```
    http://server.example.com:9180/ca/ee/ca
    ```

    b. Click the **Retrieval** tab.
    c. Click **Import CA Certificate Chain** in the left menu, and then select **Download the CA certificate chain in binary form**.
    d. When prompted, save the CA certificate chain file.
    e. In the Internet Explorer menu, click **Tools**, and select **Internet Options**.
    f. Open the **Content** tab, and click the **Certificates** button.
    g. Click the **Import** button. In the import window, browse for and select the imported certificate chain.

    The import process prompts for which certificate store to use for the CA certificate chain. Select **Automatically select the certificate store based on the type of certificate**.
    h. Once the certificate chain is imported, open the **Trusted Root Certificate Authorities** tab to verify that the certificate chain was successfully imported.
3. After the certificate chain is imported, Internet Explorer can access the secure end services pages. Open the secure site.

    ```
    https://server.example.com:9444/ca/ee/ca
    ```

4. There is probably a security exception when opening the end services pages. Add the CA services site to Internet Explorer's **Trusted Sites** list.
    a. In the Internet Explorer menu, click **Tools**, and select **Internet Options**.
    b. Open the **Security** tab, and click **Sites** to add the CA site to the trusted list.
    c. Set the **Security level for this zone** slider for the CA services page to **Medium**; if this security setting is too restrictive in the future, then try resetting it to **Medium-low**.

5. Close the browser.

To verify that Internet Explorer can be used for enrollments, try enrolling a user certificate:

1. Open the Certificate Manager's end-entities page.

```
https://server.example.com:9444/ca/ee/ca
```

2. Select the Manual User Dual-Use Certificate Enrollment form.
3. Fill in the user information, and click **Submit**.
4. If the request is successfully submitted, the CA will return a request number for the request with a message that it was successfully submitted to the CA and awaiting approval.

Chapter 2. CA: Working with Certificate Profiles

A Certificate Manager agent is responsible for approving certificate profiles that have been configured by a Certificate System administrator. Certificate Manager agents also manage and approve certificate requests that come from profile-based enrollments.

2.1. About Certificate Profiles

A certificate profile defines everything associated with issuing a certificate, including the authentication method, the authorization method, the certificate content (defaults), constraints for content values in the requested certificate type, and the contents of the input and output forms associated with the certificate profile.

There are three categories of information that constitute a certificate profile:

- *Profile inputs.* Profile inputs are parameters and values that are submitted to the CA when a certificate is requested. Profile inputs include public keys for the certificate request and the certificate subject name requested by the end entity for the certificate.
- *Profile policy sets.* A certificate profile can have one or more policy sets, each of which is defined by a set of defaults and constraints.
  - *Profile defaults.* Profile defaults are parameters and values defined by the CA administrator. Profile defaults include how long the certificate is valid and what certificate extensions appear for each type of certificate issued.
  - *Profile constraints.* Profile constraints are parameters and values that form the rules or policies for issuing certificates. Profile constraints include rules like requiring the certificate subject name to have at least one CN component, setting the validity of a certificate to a maximum of 360 days, grace periods to allow certificate renewal as the certificate nears its expiration date, or requiring that the **`subjectaltname`** extension always be set to **`true`**.
- *Profile outputs.* Profile outputs are parameters and values that specify the format in which to issue the certificate to the end entity. Profile outputs include base-64 encoded files, CMMF responses, and PKCS #7 output, which also includes the CA chain.

An administrator sets up a certificate profile by associating an existing authentication plug-in, or method, with the certificate profile; enabling and configuring defaults and constraints; and defining inputs and outputs. The administrator can use the existing certificate profiles, modify the existing certificate profiles, create new certificate profiles, and disable or delete any certificate profile that will not be used in the PKI.

Once a certificate profile is set, it appears on the **`Manage Certificate Profiles`** page of the agent services interface, where an agent can approve, and thus enable, a certificate profile. Once the certificate profile is enabled, it appears on the **`List Certificate Profile`** tab of the end-entities page, so end entities can enroll for certificates using the certificate profile.

The certificate profile enrollment or renewal page contains links to each type of certificate profile enrollment that has been enabled. When an end entity selects one of those links, an enrollment page appears, containing the enrollment form specific to that certificate profile. The enrollment page for the certificate profile in the end entities page is dynamically generated from the inputs defined for the certificate profile. If an authentication plug-in is configured, additional fields may be added that are needed to authenticate the user with that authentication method.

A manual enrollment is a request when no authentication plug-in is configured. When the end entity submits a certificate request with a manual enrollment profile, the certificate request is queued in the agent services page as a certificate enrollment request. The agent can change the request, reject it, change the status, or approve it. The agent can also update the request without submitting it or validate that the request adheres to the profile's defaults and constraints. Agents are bound by the constraints

set in the profile; they cannot change the request so that a constraint is violated. The signed approval is immediately processed, and a certificate is issued.

When a certificate profile is associated with an authentication method, the request generates a certificate automatically if the user successfully authenticates, all required information is provided, and the request does not violate any of the constraints set for the certificate profile. If an authorization method is set in the profile, a check is done to authorize the requester.

NOTE

There are several different kinds of authentication that can be used for enrollment or renewal profiles. However, some authentication methods require outside configuration to work. For example, to use a renewal profile which uses directory-based authentication, then directory-based authentication must be enabled and the CA configured to connect to an LDAP directory before that authentication module can be used.

The issued certificate contains the default content for the certificate profile (like the extensions and validity period) and follows the constraints set for each default. There can be more than one policy set. Each policy set consists of multiple sets of defaults and constraints, which defines individual policy settings. Each policy set has a unique policy ID, and every policy within the set is identified as a member of the set by using the same value for the policy set ID for each default and constraint in the set.

The server evaluates each policy set for each request it receives. When a single certificate is requested, the profile should contain a single policy set to evaluate. When dual key pairs are requested, then there must be two policies in the policy set. The first policy set is evaluated with the first certificate request, and the second set is evaluated with the second certificate request. Policies within each policy set are evaluated in the specific order set in the policy set order list.

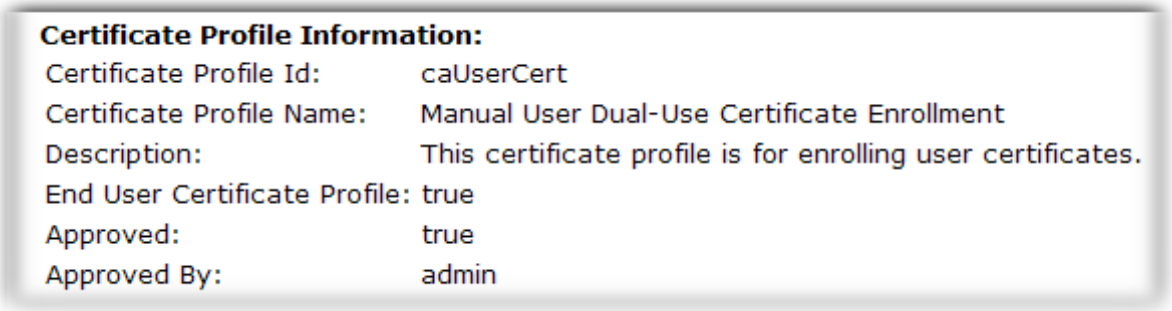
A profile usually contains inputs, policy sets, and outputs, as illustrated in the **caUserCert** profile in Section 2.2, “Example caUserCert Profile”.

2.2. Example caUserCert Profile

The first part of a certificate profile is the description. This shows the name, long description, whether it is enabled, and who enabled it.

```
desc=This certificate profile is for enrolling user certificates.
visible=true
enable=true
enableBy=admin
name=Manual User Dual-Use Certificate Enrollment
```

In the **Managing Certificate Profiles** page of the CA's agent services, this looks like:



Certificate Profile Information:

Certificate Profile Id:	caUserCert
Certificate Profile Name:	Manual User Dual-Use Certificate Enrollment
Description:	This certificate profile is for enrolling user certificates.
End User Certificate Profile:	true
Approved:	true
Approved By:	admin

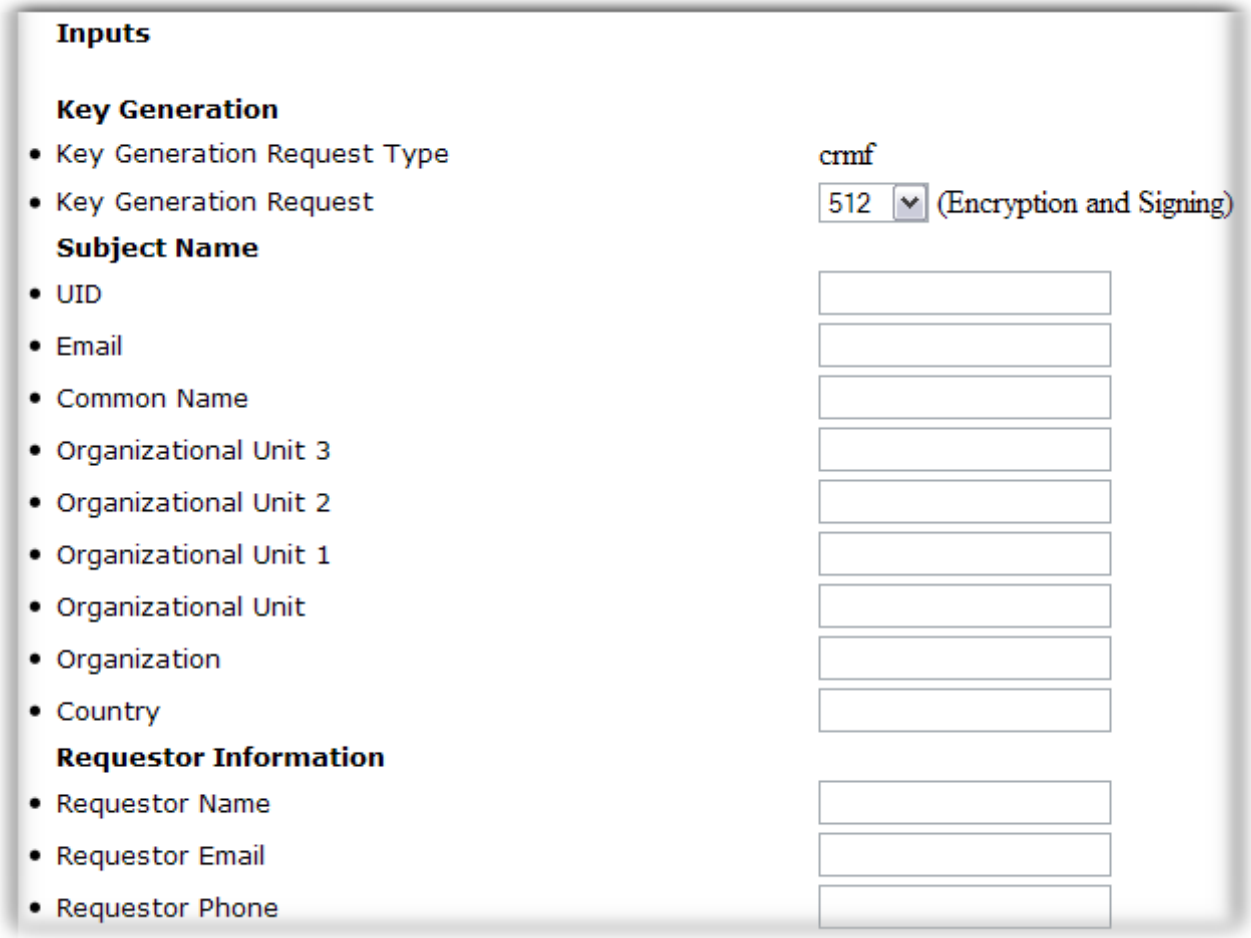
Next, the profile lists all of the required inputs for the profile:

```
input.list=i1,i2,i3
input.i1.class_id=keyGenInputImpl
input.i2.class_id=subjectNameInputImpl
input.i3.class_id=submitterInfoInputImpl
```

For the **`caUserCert`** profile, this defines the keys to generate, the fields to use in the subject name, and the fields to use for the person submitting the certificate.

- *Key generation* specifies that the key pair generation during the request submission be CRMF-based. A drop-down menu sets the key-size for the keys.
- *Subject name* is used when distinguished name (DN) parameters need to be collected from the user; the user DN can be used to create the subject name in the certificate.
  - UID (for the user in the LDAP directory)
  - Email
  - Common name
  - Organizational unit
  - Organization
  - Country
- *Requester*. This input has three form fields:
  - Requester name
  - Requester email
  - Requester phone

The inputs are listed in the certificate enrollment page for end entities, not the profile configuration page for agents:



The profile next must define the output, meaning the format of the final certificate. There are several pre-defined outputs. More than one of these can be used, but none of the values of the output can be modified.

```
output.list=o1
output.o1.class_id=certOutputImpl
```

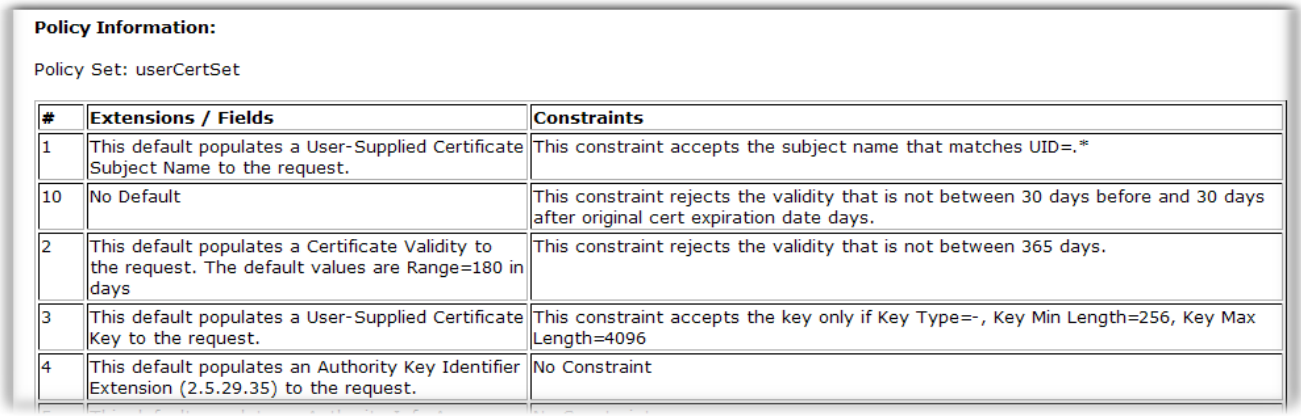
For **`caUserCert`**, the output displays the certificate in pretty print format. This output needs to be specified for any automated enrollment. Once a user successfully authenticates using the automated enrollment method and is authorized to receive the certificate, the certificate is automatically generated, and this output page is returned to the user. In an agent-approved enrollment, the user can get the certificate, once it is issued, by providing the request ID in the CA end entities page.

The last — largest — block of configuration is the policy set for the profile. Policy sets list all of the settings that are applied to the final certificate, like its validity period, its renewal settings, and the actions the certificate can be used for. The **`policyset.list`** parameter identifies the block name of the policies applied to the certificate; the **`policyset.userCertSet.list`** lists the individual policies to apply.

For example, the sixth policy populates the Key Usage Extension automatically in the certificate, according to the configuration in the policy. It sets the defaults and requires the certificate to use those defaults by setting the constraints:

```
policyset.list=userCertSet
policyset.userCertSet.list=1,10,2,3,4,5,6,7,8,9
...
policyset.userCertSet.6.constraint.class_id=keyUsageExtConstraintImpl
policyset.userCertSet.6.constraint.name=Key Usage Extension Constraint
policyset.userCertSet.6.constraint.params.keyUsageCritical=true
policyset.userCertSet.6.constraint.params.keyUsageDigitalSignature=true
policyset.userCertSet.6.constraint.params.keyUsageNonRepudiation=true
policyset.userCertSet.6.constraint.params.keyUsageDataEncipherment=false
policyset.userCertSet.6.constraint.params.keyUsageKeyEncipherment=true
policyset.userCertSet.6.constraint.params.keyUsageKeyAgreement=false
policyset.userCertSet.6.constraint.params.keyUsageKeyCertSign=false
policyset.userCertSet.6.constraint.params.keyUsageCrlSign=false
policyset.userCertSet.6.constraint.params.keyUsageEncipherOnly=false
policyset.userCertSet.6.constraint.params.keyUsageDecipherOnly=false
policyset.userCertSet.6.default.class_id=keyUsageExtDefaultImpl
policyset.userCertSet.6.default.name=Key Usage Default
policyset.userCertSet.6.default.params.keyUsageCritical=true
policyset.userCertSet.6.default.params.keyUsageDigitalSignature=true
policyset.userCertSet.6.default.params.keyUsageNonRepudiation=true
policyset.userCertSet.6.default.params.keyUsageDataEncipherment=false
policyset.userCertSet.6.default.params.keyUsageKeyEncipherment=true
policyset.userCertSet.6.default.params.keyUsageKeyAgreement=false
policyset.userCertSet.6.default.params.keyUsageKeyCertSign=false
policyset.userCertSet.6.default.params.keyUsageCrlSign=false
policyset.userCertSet.6.default.params.keyUsageEncipherOnly=false
policyset.userCertSet.6.default.params.keyUsageDecipherOnly=false
...
```

The policy sets are summarized on the agent services **`Managing Certificate Profiles`** page.



Policy Information:

Policy Set: userCertSet

#	Extensions / Fields	Constraints
1	This default populates a User-Supplied Certificate Subject Name to the request.	This constraint accepts the subject name that matches UID=.*
10	No Default	This constraint rejects the validity that is not between 30 days before and 30 days after original cert expiration date days.
2	This default populates a Certificate Validity to the request. The default values are Range=180 in days	This constraint rejects the validity that is not between 365 days.
3	This default populates a User-Supplied Certificate Key to the request.	This constraint accepts the key only if Key Type=-, Key Min Length=256, Key Max Length=4096
4	This default populates an Authority Key Identifier Extension (2.5.29.35) to the request.	No Constraint

2.3. List of Certificate Profiles

The following pre-defined certificate profiles are ready to use when the Certificate System CA is installed. These certificate profiles have been designed for the most common types of certificates, and they provide common defaults and constraints, authentication methods, authorization methods, and inputs and outputs. These profiles can be edited or new profiles added as necessary.

Table 2.1. List of Certificate Profiles

Profile ID	Profile Name	Description
caAdminCert	Security Domain Administrator Certificate Enrollment	Enrolls Security Domain Administrator's certificates with LDAP authentication against the internal LDAP database.
caAgentFileSigning	Agent-Authenticated File Signing	This certificate profile is for file signing with agent authentication.
caAgentServerCert	Agent-Authenticated Server Certificate Enrollment	Enrolls server certificates with agent authentication.
caCACert	Manual Certificate Manager Signing Certificate Enrollment	Enrolls Certificate Authority certificates.
caCMCUserCert	Signed CMC-Authenticated User Certificate Enrollment	Enrolls user certificates by using the CMC certificate request with CMC Signature authentication.
caDirUserCert	Directory-Authenticated User Dual-Use Certificate Enrollment	Enrolls user certificates with directory-based authentication.
caDirUserRenewal	Directory-Authenticated User Certificate Self-Renew profile	Renews user certificates, with directory-based authentication.
caDualCert	Manual User Signing & Encryption Certificates Enrollment	Enrolls dual user certificates. It works only with Netscape 7.0 or later.
caDualRAuserCert	RA Agent-Authenticated User Certificate Enrollment	Enrolls user certificates with RA agent authentication.
caFullCMCUserCert	Signed CMC-Authenticated User Certificate Enrollment	Enrolls user certificates by using the CMC certificate request with CMC Signature authentication.
caInstallCACert	Manual Security Domain Certificate Authority Signing Certificate Enrollment	Enrolls Security Domain Certificate Authority certificates.
caInternalAuthAuditSigningCert	Audit Signing Certificate Enrollment	Enrolls a signing certificate to use for signing audit logs; used automatically during any subsystem configuration, with the exception of the RA.
caInternalAuthDRMstorageCert	Security Domain DRM Storage Certificate Enrollment	Enrolls DRM storage certificates for DRMs within a security domain; used automatically during a DRM configuration.
caInternalAuthOCSPCert	Security Domain OCSP Manager Signing Certificate Enrollment	Enrolls Security Domain OCSP Manager certificates.
caInternalAuthServerCert	Security Domain Server Certificate Enrollment	Enrolls Security Domain server certificates.
caInternalAuthSubsystemCert	Security Domain Subsystem Certificate Enrollment	Enrolls Security Domain subsystem certificates.

caInternalAuthTransportCert	Security Domain Data Recovery Manager Transport Certificate Enrollment	Enrolls Security Domain Data Recovery Manager transport certificates.
caManualRenewal	Renew certificate to be manually approved by agents	Renews a certificate, with manual agent approval.
caOCSPCert	Manual OCSP Manager Signing Certificate Enrollment	Enrolls OCSP Manager certificates.
caOtherCert	Other Certificate Enrollment	Enrolls other certificates.
caRAagentCert	RA Agent-Authenticated Agent User Certificate Enrollment	Enrolls RA agent user certificates with RA agent authentication.
caRACert	Manual Registration Manager Signing Certificate Enrollment	Enrolls Registration Manager certificates.
caRARouterCert	RA Agent-Authenticated Router Certificate Enrollment	Enrolls router certificates after agent approval (as opposed to automatic enrollment).
caRAserverCert	RA Agent-Authenticated Server Certificate Enrollment	Enrolls server certificates with RA agent authentication.
caRouterCert	One Time Pin Router Certificate Enrollment	Enrolls router certificates using an automatically-generated, one-time PIN that the router can use to retrieve its certificate.
caServerCert	Manual Server Certificate Enrollment	Enrolls server certificates.
caSignedLogCert	Manual Log Signing Certificate Enrollment	Enrolls audit log signing certificates.
caSimpleCMCUserCert	Simple CMC Enrollment	Enrolls user certificates by using the CMC certificate request with CMC Signature authentication.
caSSLClientSelfRenewal	Self-renew user SSL client certificates	Renews certificates using certificate-base authentication.
caTempTokenDeviceKeyEnrollment	Temporary Device Certificate Enrollment	Enrolls temporary keys to be used by servers or other network devices on a token; used by the TPS for smart card enrollment operations. These are temporary keys, valid for about a week, and intended to replace a temporarily lost token.
caTempTokenUserEncryptionKeyEnrollment	Temporary Token User Encryption Certificate Enrollment	Enrolls an encryption key on a token; used by the TPS for smart card enrollment operations. These are temporary keys, valid for about a week, and intended to replace a temporarily lost token.
caTempTokenUserSigningKeyEnrollment	Temporary Token User Signing Certificate Enrollment	Enrolls a signing key on a token; used by the TPS for smart card enrollment operations. These

		are temporary keys, valid for about a week, and intended to replace a temporarily lost token.
caTokenDeviceKeyEnrollment	Token Device Key Enrollment	Enrolls keys to be used by servers or other network devices on a token; used by the TPS for smart card enrollment operations.
caTokenMSLoginEnrollment	Token User MS Login Certificate Enrollment	Enrolls key to be used by a person for logging into a Windows domain or PC; used by the TPS for smart card enrollment operations.
caTokenUserEncryptionKeyEnrollment	Token User Encryption Certificate Enrollment	Enrolls an encryption key on a token; used by the TPS for smart card enrollment operations.
caTokenUserEncryptionKeyRenewal	smart card token encryption cert renewal profile	Renews an encryption key that was enrolled on a token using the caTokenUserEncryptionKeyEnrollment profile; used by a TPS subsystem.
caTokenUserSigningKeyEnrollment	Token User Signing Certificate Enrollment	Enrolls a signing key on a token; used by the TPS for smart card enrollment operations.
caTokenUserSigningKeyRenewal	smart card token signing cert renewal profile	Renews a signing that was enrolled on a token using the caTokenUserSigningKeyEnrollment profile; used by a TPS subsystem.
caTPSCert	Manual TPS Server Certificate Enrollment	Enrolls TPS server certificates.
caTransportCert	Manual Data Recovery Manager Transport Certificate Enrollment	Enrolls Data Recovery Manager transport certificates.
caUserCert	Manual User Dual-Use Certificate Enrollment	Enrolls user certificates.
caUUIDdevicecert	Manual device Dual-Use Certificate Enrollment to contain UUID in SAN	Enrolls certificates for devices which must contain a unique user ID number (UUID) as a component in the certificate's subject alternate name extension.
DomainController	Domain Controller	Enrolls certificates to be used by a Windows domain controller.

2.4. Enabling and Disabling Certificate Profiles

Any certificate profiles that have been configured by an administrator are listed in the **Manage**

Certificate Profiles page of the agent services page, which is accessed through the **Manage Certificate Profiles** link in the left menu of the CA agent services page.

The **Manage Certificate Profiles** page contains all of the certificate profiles that have been set up by an administrator. It shows the name of the certificate profile, a short description of the certificate profile, whether this is an end user certificate profile, whether the certificate profile has been approved and enabled, and, if approved, which agent user ID approved the request.

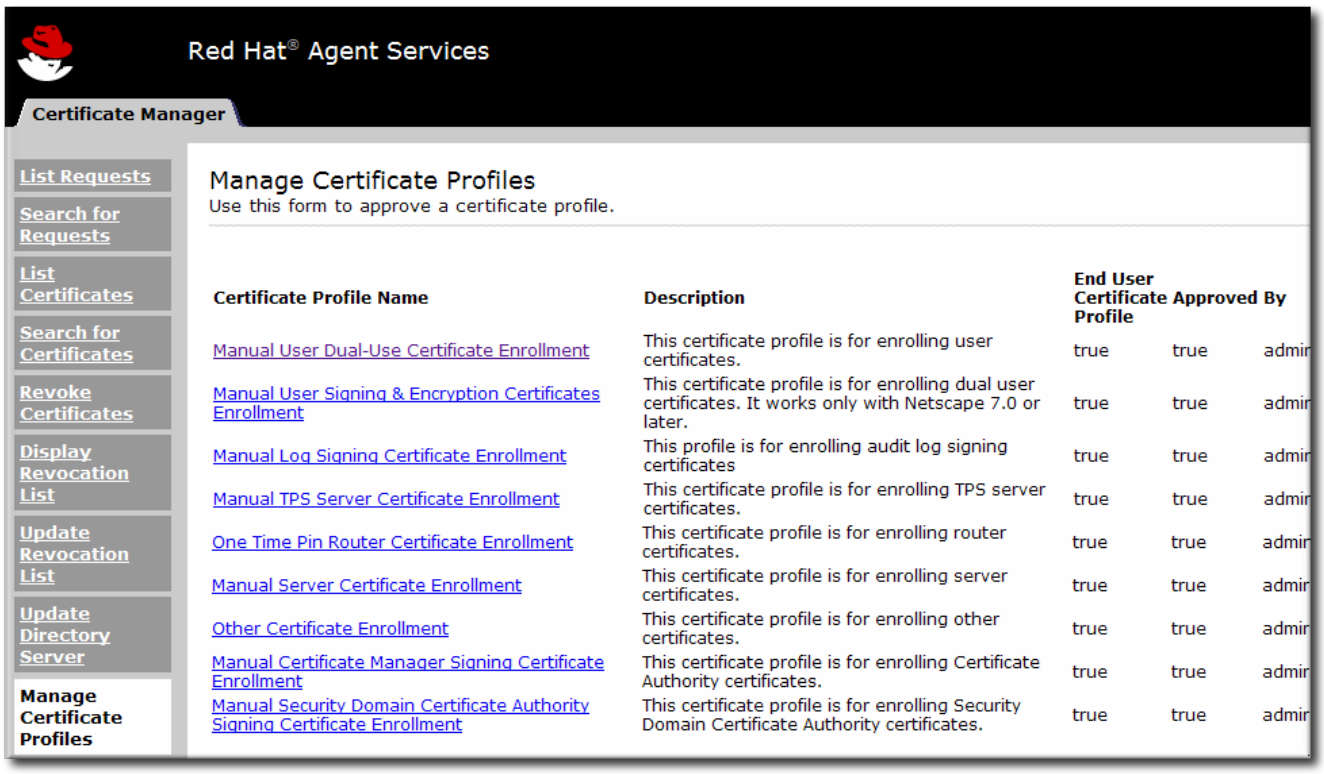


Figure 2.1. List of Certificate Profiles

2.4.1. Viewing Certificate Profile Information

Information about any certificate profile is available by clicking the name of the certificate profile, which is linked to the **Approve Certificate Profile** page. This page lists information about the certificate profile and allows an agent to approve a certificate profile or disable a previously-approved certificate profile. An approved certificate profile can only be disabled by the agent who originally approved it.

To view a profile, open its **Approve Certificate Profile** page:

1. Click the **Manage Certificate Profiles** link in the left menu.
2. Click the profile name in the list of profiles.

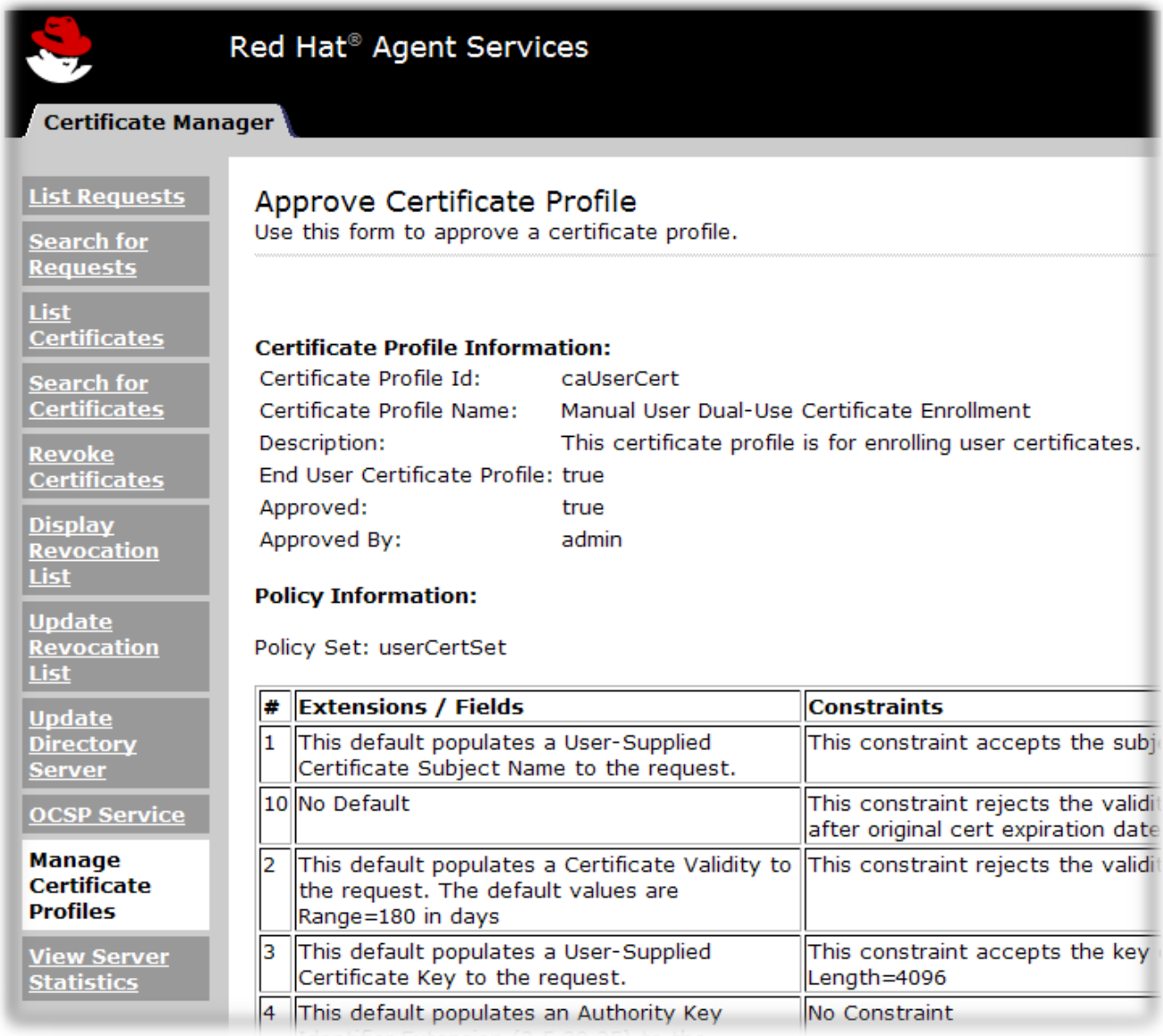

Red Hat® Agent Services
Certificate Manager
List Requests
Search for Requests
List Certificates
Search for Certificates
Revoke Certificates
Display Revocation List
Update Revocation List
Update Directory Server
OCSP Service
Manage Certificate Profiles
View Server Statistics
Approve Certificate Profile
Use this form to approve a certificate profile.
Certificate Profile Information:
Certificate Profile Id: caUserCert
Certificate Profile Name: Manual User Dual-Use Certificate Enrollment
Description: This certificate profile is for enrolling user certificates.
End User Certificate Profile: true
Approved: true
Approved By: admin
Policy Information:
Policy Set: userCertSet
Extensions / Fields Constraints
1 This default populates a User-Supplied Certificate Subject Name to the request. This constraint accepts the subj
10 No Default This constraint rejects the validi after original cert expiration date
2 This default populates a Certificate Validity to the request. The default values are Range=180 in days This constraint rejects the validi
3 This default populates a User-Supplied Certificate Key to the request. This constraint accepts the key Length=4096
4 This default populates an Authority Key No Constraint

Figure 2.2. Profile Page

If the **End User** field of the certificate profile is marked true, then this certificate profile appears as an enrollment form in the end entities page. If the **End User** field of the certificate profile is marked false, then this certificate profile does not appear in the end entities page. This parameter determines whether the certificate profile needs to be received from the end entities page in order to be processed.

Each policy has a policy information section which shows a table for each policy set. A certificate profile usually has one policy set. If the enrollment is for dual key pairs, then there are two policy sets, one for the signing certificate and one for the encryption certificate. The policy set defines all of the defaults and constraints that have been set for the requested certificate. For dual key pairs, two certificates are requested, one for the signing key and one for the encryption key.

The policy set table in the policy information sections contains the following information for the policy set:

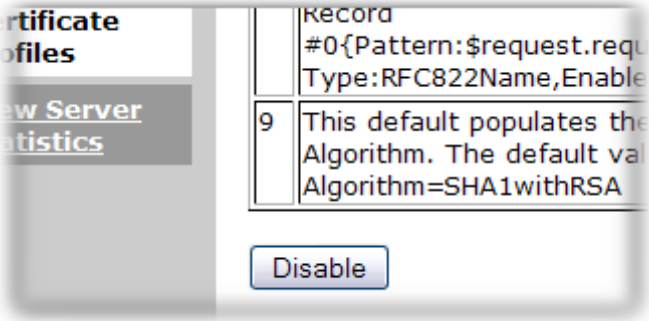
- *#.* The policy ID number (#) for this set of defaults and constraints.
- *Defaults [Extensions/Fields].* The defaults set to define certificate content, including extensions.
- *Constraints.* The constraints placed on the certificate content. The certificate content in the requested certificate must comply with these constraints in order to be issued. If the constraint value

is left blank or is set to a dash (**-**), then applying the constraint is optional, and the issued certificate is not constrained.

2.4.2. Enabling or Disabling a Certificate Profile

To enable (approve) or disable a certificate profile:

1. Go to the **Manage Certificate Profiles** page, and click on a certificate profile name.
2. Open the **Approve Certificate Profile** page for that certificate profile.
3. Click the **Approve** button at the bottom of the page to enable the profile or **Disable** to disable it.



NOTE

It is only possible to disable a certificate profile after it has been approved. New profiles are disabled by default and must be enabled before they can be used.

After a certificate profile is approved, it appears in the end entities page, which allows an end entity to use that certificate profile to enroll for a certificate. Likewise, once a certificate profile is disabled, it is no longer available in the end entities page for end entities to use to enroll for certificates.

NOTE

When a certificate profile is enabled, administrators cannot change any aspect of the certificate profile. The certificate profile must first be disabled before an administrator to modify the certificate profile.

Chapter 3. CA: Handling Certificate Requests

A Certificate Manager agent is responsible for handling both manual enrollment requests made by end entities (end users, server administrators, and other Certificate System subsystems) and automated enrollment requests that have been deferred. This chapter describes the general procedure for handling requests and explains how to handle different aspects of certificate request management.

3.1. Managing Requests

The procedure for handling certificate enrollment requests is as follows:

1. View the list of pending requests for the Certificate Manager (see Section 3.2, “Listing Certificate Requests”).
2. Select a request from the list (see Section 3.2.1, “Selecting a Request”).
3. Process the request (see Section 3.2.2, “Searching for Certificates (Advanced)” and Section 3.3, “Approving Requests”).

Processing a certificate request for a certificate allows one of several actions, listed in Table 3.1, “Possible Agent Actions for Certificate Requests”.

Table 3.1. Possible Agent Actions for Certificate Requests

Action	Description
Approve the request	A request can be approved manually by an agent or automatically by the certificate profile if the request has been authenticated and if the system has been configured to allow automatic enrollment. After a request has been approved, the Certificate System issues the requested certificate. The end user can be automatically notified that the certificate was issued.
Reject the request	A certificate request can be rejected manually or automatically by the certificate profile if the request does not conform to the profile's defaults and constraints. If automatic notification is configured, a notification is automatically sent to the requester when the certificate request is rejected.
Cancel the request	A request can be canceled manually, but requests can never be canceled automatically. Users do not receive automatic notification of canceled requests. Cancellation can be useful if the user has left the company since submitting the request or if the user has already been contacted about a problem with the certificate request and, therefore, does not need to be notified.
Update the request	A pending certificate request can be updated by changing some of its values, such as the subject name. The different default values associated with a certificate profile changed by the agent only results in the certificate request values being changed but does not change its state.
Validate the request	A request that uses a certificate profile can be checked, or validated, to see if the request complies with the defaults and constraints set by the certificate profile. This action only checks the request but does not submit or edit the request.
Assign the request	A certificate request can be manually assigned by the agent processing the request to himself. Requests cannot be assigned to another agent.
Unassign the request	A request can be removed from an agent's queue if necessary, such as when requests are assigned to an agent who has since left the company.

Approving, canceling, and rejecting certificate requests all alter the request status. Assigning, unassigning, updating, and validating certificate requests do not alter the request status. If the form is closed without taking one of these actions, the request remains in the queue with the same status.

Figure 3.1, “Certificate Request Management Process” illustrates the process for handling requests and the different types of status for a request.

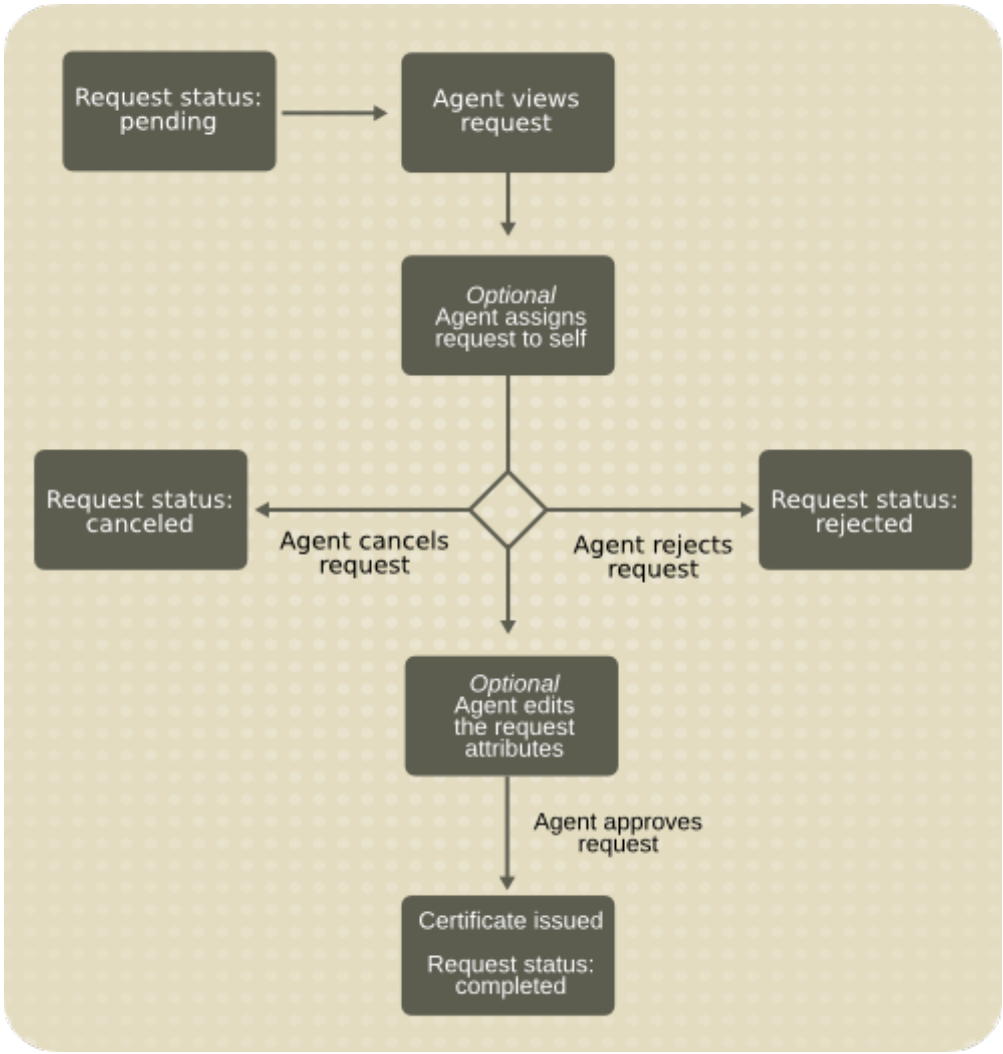


Figure 3.1. Certificate Request Management Process

3.2. Listing Certificate Requests

The Certificate Manager keeps a queue of all certificate service requests that have been submitted to it. The queue records whether a request is pending, completed, canceled, or rejected. Three types of requests can be in the queue:

- Certificate enrollment requests
- Certificate renewal requests
- Certificate revocation requests

A Certificate Manager agent must review and approve manual enrollment requests. Certificate requests that require review have a status of *pending*.

To see a list of requests:

1. Go to the Certificate Manager agent services page.

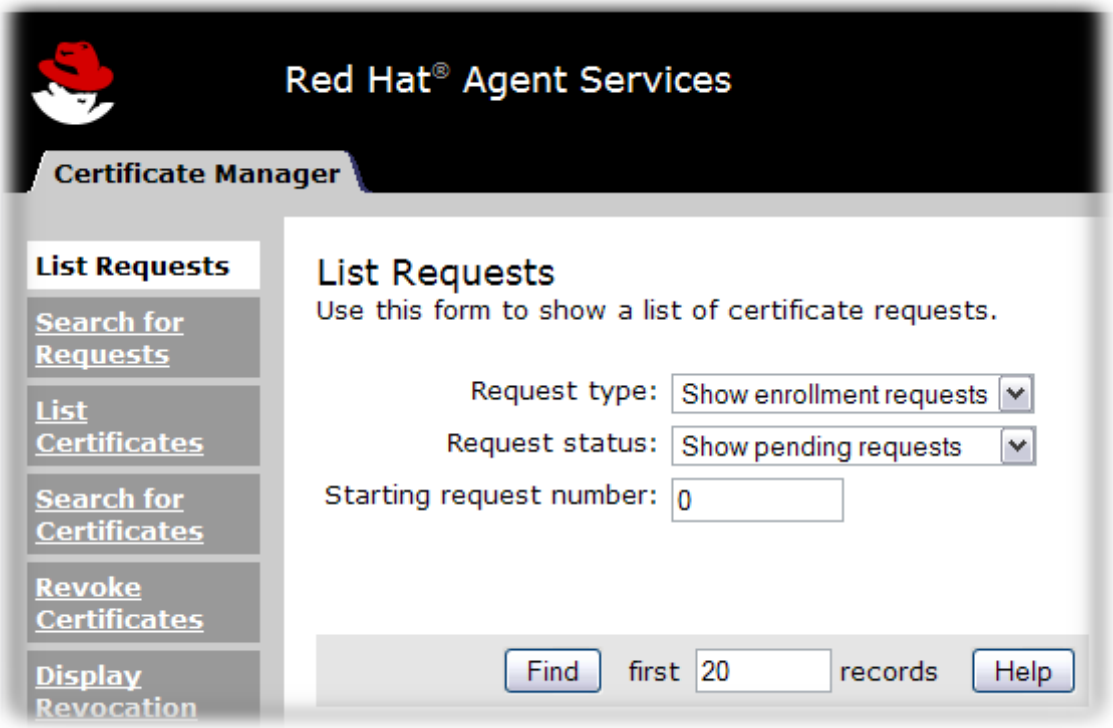
```
https://server.example.com:9443/ca/agent/ca
```

NOTE

An agent must have the proper client certificate to access this page.

2. Click **`List Requests`** to view the queue of certificates requests.

   The **`List Requests`** form appears.



3. View certificate requests request type by selecting one of the options from the **Request type** menu.
   - Show enrollment requests
   - Show renewal requests
   - Show revocation requests
   - Show all requests
4. View requests by request status by selecting one of the options in the **Request status** menu.
   - *Show pending requests.* These are enrollment requests that have not yet been processed but are waiting for manual review.
   - *Show canceled requests.* These are requests that have been manually canceled by an agent. Users do not receive automatic notification of canceled requests. Cancellation can be useful if the user has left the company since submitting the request or if the user has already been contacted about a problem and does not need to be notified about the request status.
   - *Show rejected requests.* These are requests that have been either manually rejected or rejected automatically during profile processing. If the system has been configured to provide automatic notifications to users, a notice is sent to the requester when the request is rejected.
   - *Show completed requests.* These are requests that have been completed, including issued certificates and completed revocation requests.
   - *Show all requests.* This shows all requests of the selected type, regardless of status.
5. To start the list at a specific place in the queue, enter the starting request identifier in decimal or hexadecimal form. Use **`0x`** to indicate a hexadecimal number; for example, **`0x2A`**.
6. Choose the number of matching requests to be returned. When a number is specified, the system

displays that number of certificate requests, beginning with the starting sequence number that matches the specified criteria.

7. Click **Find** to display the list of requests that match the specified criteria.

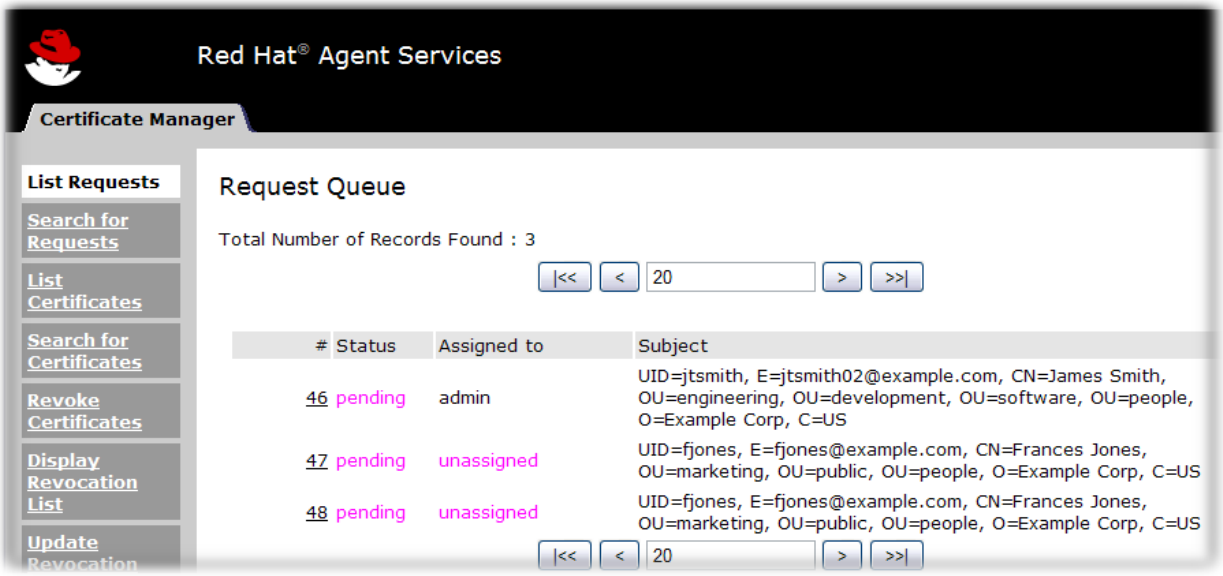

Red Hat® Agent Services
Certificate Manager
List Requests
Search for Requests
List Certificates
Search for Certificates
Revoke Certificates
Display Revocation List
Update Revocation
Request Queue
Total Number of Records Found : 3
|<<
<
20
>
>>|
Status Assigned to Subject
46 pending admin UID=jtsmith, E=jtsmith02@example.com, CN=James Smith, OU=engineering, OU=development, OU=software, OU=people, O=Example Corp, C=US
47 pending unassigned UID=fjones, E=fjones@example.com, CN=Frances Jones, OU=marketing, OU=public, OU=people, O=Example Corp, C=US
48 pending unassigned UID=fjones, E=fjones@example.com, CN=Frances Jones, OU=marketing, OU=public, OU=people, O=Example Corp, C=US
|<<
<
20
>
>>|

Figure 3.2. Request Queue

3.2.1. Selecting a Request

To select a request from the queue:

1. On the agent services page, click **List Requests**, specify search criteria, and click **Find** to display a list of certificate signing requests.
2. Select a request to examine from the **Request Queue** form.
3. If a desired request not shown, scroll to the bottom of the list, specify an additional number of requests to be listed, and click **Find**. That number of additional requests matching original search criteria is shown.
4. When the request has been found, click **Details**.
5. The **Request Details** form appears, showing detailed information about the selected request. Use this form to approve or manage the request.

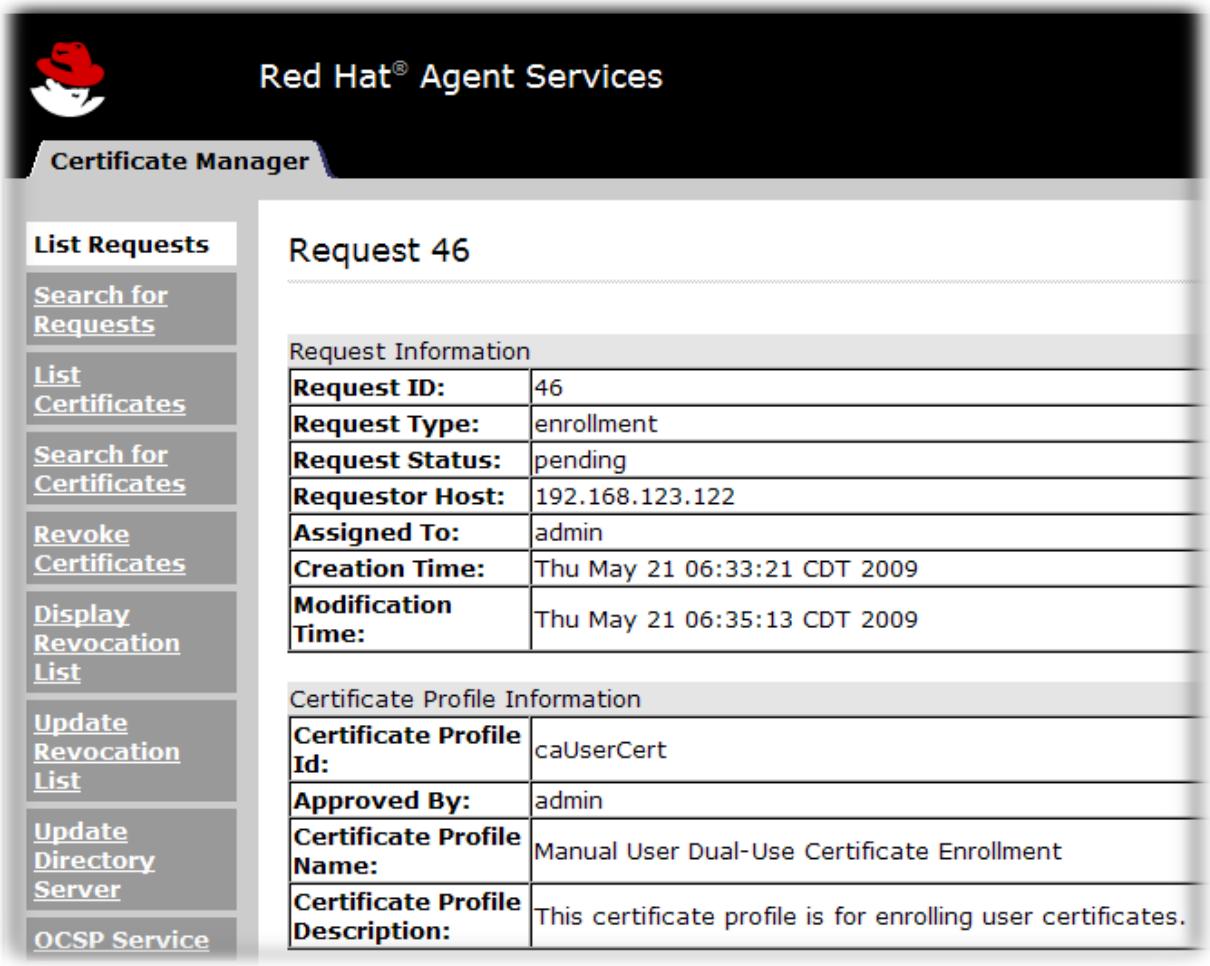


Figure 3.3. Request Details

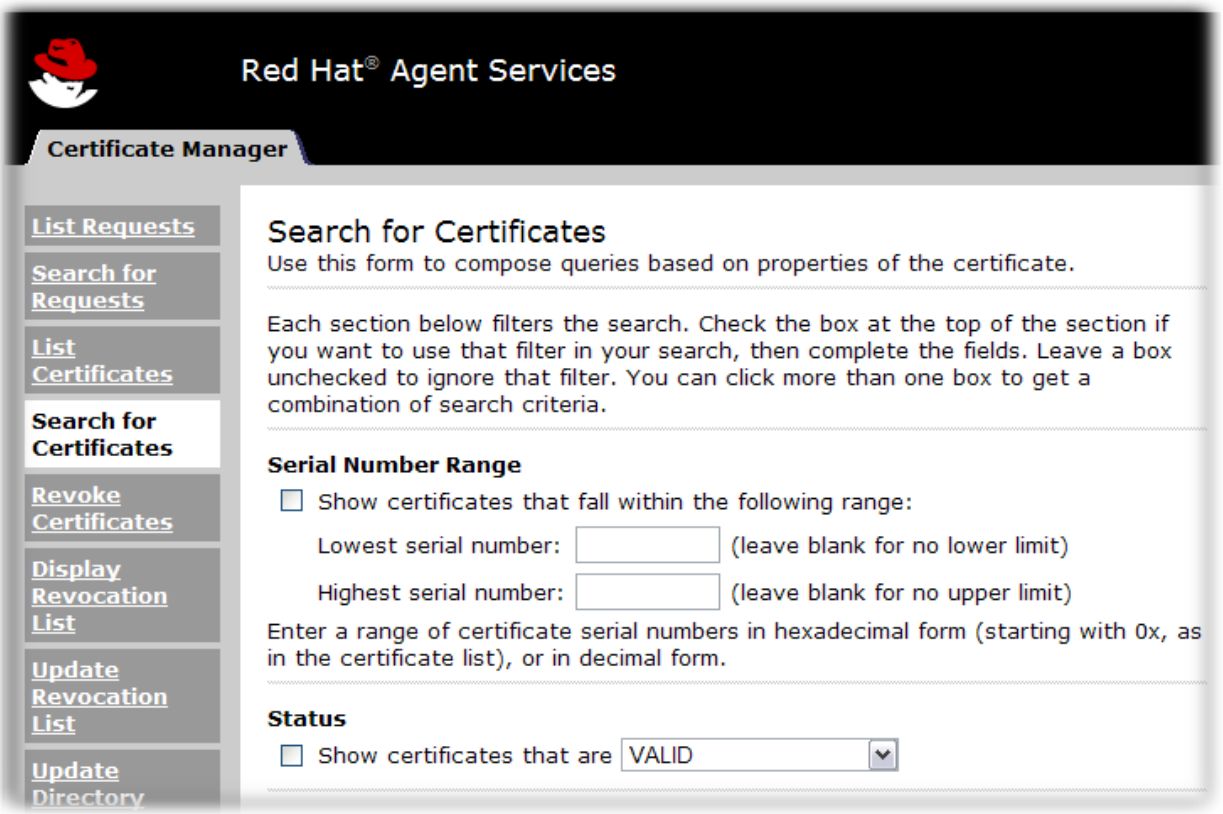
NOTE

If the system changes the state of the displayed request, using the browser's **Back** or **Forward** buttons or history to navigate can cause the data display to become out of date. To refresh the data, click the highlighted serial number at the top of the page.

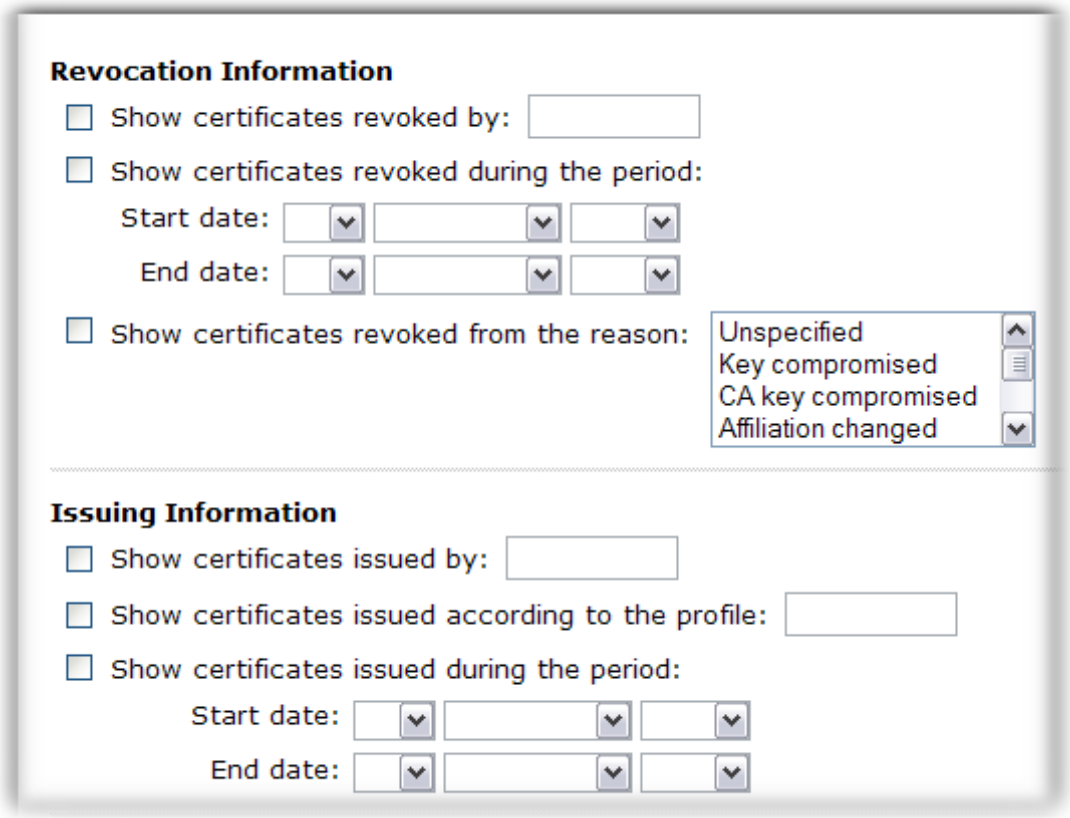
3.2.2. Searching for Certificates (Advanced)

Search for certificates by more complex criteria than serial number using the advanced search form. To perform an advanced search for certificates:

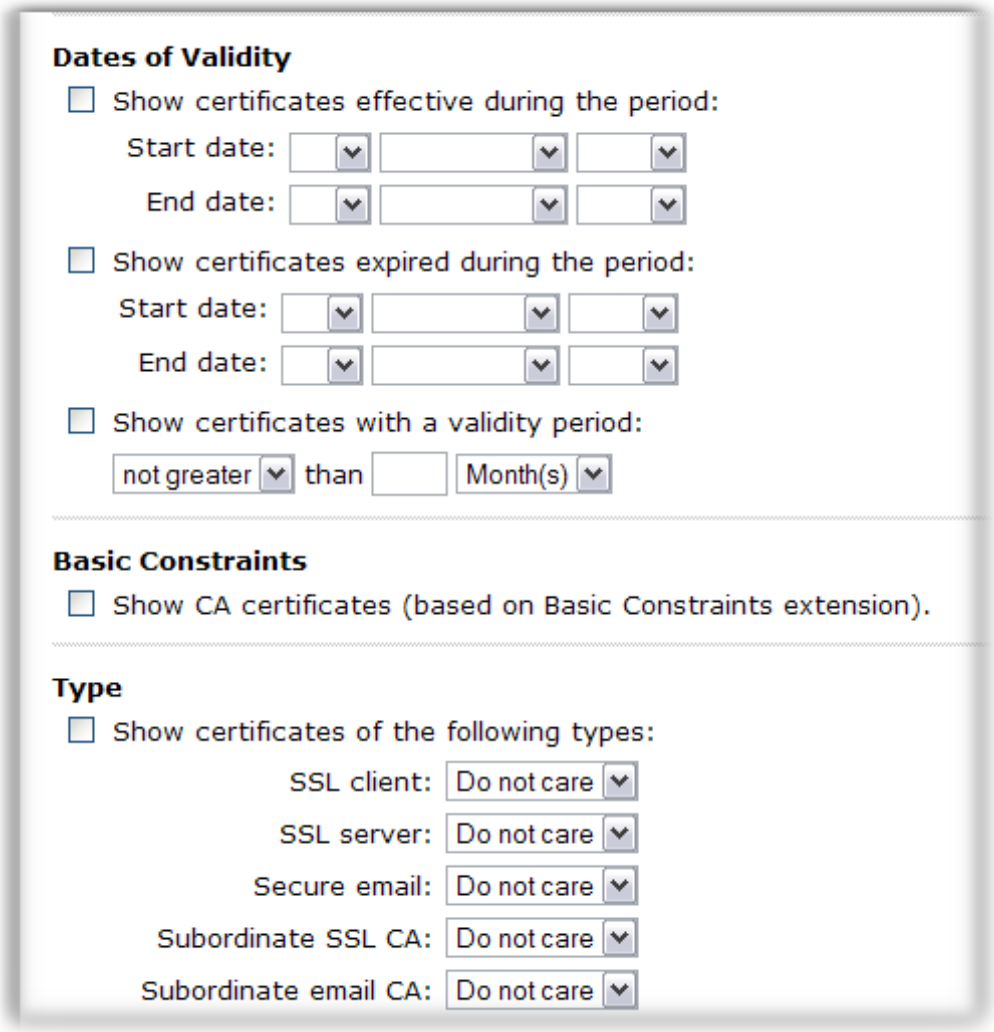
1. Open the Certificate Manager agent services page. The agent must submit the proper client certificate to access this page.
2. Click **Search for Certificates** to display the **Search for Certificates** form to specify search criteria.
3. To search by particular criteria, use one or more of the sections of the **Search for Certificates** form. To use a section, select the check box, then fill in any necessary information.


Red Hat® Agent Services
Certificate Manager
List Requests
Search for Requests
List Certificates
Search for Certificates
Revoke Certificates
Display Revocation List
Update Revocation List
Update Directory
Search for Certificates
Use this form to compose queries based on properties of the certificate.
Each section below filters the search. Check the box at the top of the section if you want to use that filter in your search, then complete the fields. Leave a box unchecked to ignore that filter. You can click more than one box to get a combination of search criteria.
Serial Number Range
Show certificates that fall within the following range:
Lowest serial number:
(leave blank for no lower limit)
Highest serial number:
(leave blank for no upper limit)
Enter a range of certificate serial numbers in hexadecimal form (starting with 0x, as in the certificate list), or in decimal form.
Status
Show certificates that are
VALID

- *Serial Number Range.* Finds a certificate with a specific serial number or lists all certificates within a range of serial numbers.
  - To find a certificate with a specific serial number, enter the serial number in both the upper limit and lower limit fields in either decimal or hexadecimal. Use **`0x`** to indicate the beginning of a hexadecimal number, such as **`0x2A`**. Serial numbers are displayed in hexadecimal form in the **`Search Results`** and **`Details`** pages.
  - To find all certificates within a range of serial numbers, enter the upper and lower limits of the serial number range in decimal or hexadecimal. Leaving either the lower limit or upper limit field blank returns all certificates before or after the number specified.
- *Status.* Selects certificates by their status. A certificate has one of the following status codes:
  - *Valid.* A valid certificate has been issued, its validity period has begun but not ended, and it has not been revoked.
  - *Invalid.* An invalid certificate has been issued, but its validity period has not yet begun.
  - *Revoked.* The certificate has been revoked.
  - *Expired.* An expired certificate has passed the end of its validity period.
  - *Revoked and Expired.* The certificate has passed its validity period and been revoked.
- *Revocation Information.* Lists certificates that have been revoked during a particular period or by a particular agent. For example, an agent can list all certificates revoked between July 2005 and April 2006 or all certificates revoked by the agent with the username **`admin`**.
  - To list certificates revoked within a time period, select the day, month, and year from the drop-down lists to identify the beginning and end of the period.
  - To list certificates revoked by a particular agent, enter the name of the agent; it is possible to use wildcards in this field.



- *Issuing Information.* Lists certificates that have been issued during a particular period or by a particular agent. For example, an agent can list all certificates issued between July 2005 and April 2006 or all certificates issued by the agent with the username **`betatest`**.
  - To list certificates issued within a time period, select the day, month, and year from the drop-down lists to identify the beginning and end of the period.
  - To list certificates issued by a particular agent, enter the name of the agent; it is possible to use wildcards in this field.
- *Dates of Validity.* List certificates that become effective or expire during a particular period. For example, an agent can list all certificates that became valid on June 1, 2003, or that expired between January 1, 2006, and June 1, 2006.



It is also possible to list certificates that have a validity period of a certain length of time, such as all certificates that are valid for less than one month.

- To list certificates that become effective or expire within a time period, select the day, month, and year from the drop-down lists to identify the beginning and end of the period.
- To list certificates that have a validity period of a certain length in time, select **Not greater than** or **Not less than** from the drop-down list, enter a number, and select a time unit from the drop-down list: days, weeks, months, or years.

- *Basic Constraints.* Shows CA certificates that are based on the Basic Constraints extension.
- *Type.* Lists certain types of certificates, such as all certificates for subordinate CAs. This search works only for certificates containing the Netscape Certificate Type extension, which stores type information. For each type, choose from the drop-down list to find certificates where that type is **On**, **Off**, or **Do Not Care**.

4. To find a certificate with a specific subject name, use the **`Subject Name`** section. Select the check box, then enter the subject name criteria. Enter values for the included search criteria and leave the others blank.

Subject Name
Show certificates with a subject name matching the following:
Email address:
Common name:
User ID:
Organization unit:
Organization:
Locality:
State:
Country:
Match Method:
Exact
Partial
Enter values for the fields you want to have in your search criteria. Leave other fields blank.
Exact match method finds certificates for subjects whose name consists exactly of the components that you have filled in above, and contains none of the components you have left blank. Pattern matching wildcard values cannot be used in this search.
Partial match method finds certificates for subjects whose name consists in part of the components you have specified above, and in addition may contain arbitrary values for the other components you have left blank above. Pattern matching wildcard values can be used in this search.

The standard tags or components are as follows:

- *Email address.* Narrows the search by email address.
- *Common name.* Finds certificates associated with a specific person or server.
- *UserID.* Searches certificates by the user ID for the person to whom the certificate belongs.
- *Organization unit.* Narrows the search to a specific division, department, or unit within an organization.
- *Organization.* Narrows the search by organization.
- *Locality.* Narrows the search by locality, such as the city.
- *State.* Narrows the search by state or province.
- *Country.* Narrows the search by country; use the two-letter country code, such as **US**.

NOTE

Certificate System certificate request forms support all UTF-8 characters for the common name and organizational unit fields. The common name and organization unit fields are included in the subject name of the certificate. This means that the searches for subject names or those elements in the subject name support UTF-8 characters.
This support does not include supporting internationalized domain names, such as in email addresses.

After entering the field values for the server to match, specify the type of search to perform:

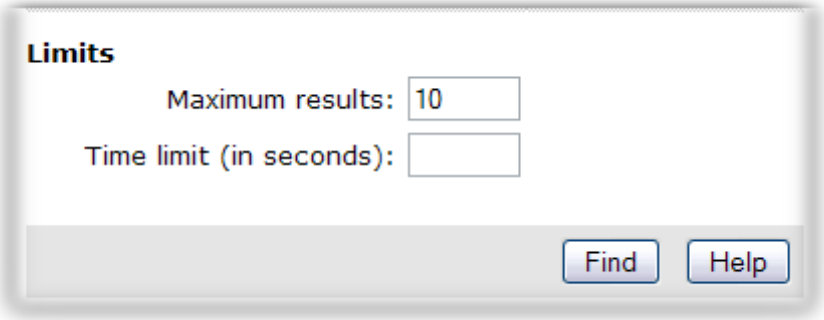
- Exact searches for certificate subject names match the exact components specified and contain none of the components left blank. Wildcards cannot be used in this type of search.
- Partial searches for certificate subject names match the specified components, but the returned certificates may also contain values in components that were left blank. Wildcard patterns can be used in this type of search by using a question mark (**?**) to match an arbitrary single character and an asterisk (*****) to match an arbitrary string of characters.

NOTE

Placing a single asterisk in a search field means that the component must be in the certificate's subject name but may have any value. Leave the field blank if it does not matter if the field is present.

5. After entering the search criteria, scroll to the bottom of the form, and enter the number of certificates matching the specified criteria that should be returned.

   Setting the number of certificates to be returned returns the first certificates found that match the search criteria up to that number. It is also possible to put a time limit on the search in seconds.



6. Click **Find**.
7. The **Search Results** form appears, showing a list of the certificates that match the search criteria. Select a certificate in the list to examine it in more detail. For more information, refer to Section 4.3, “Examining Certificate Details”.

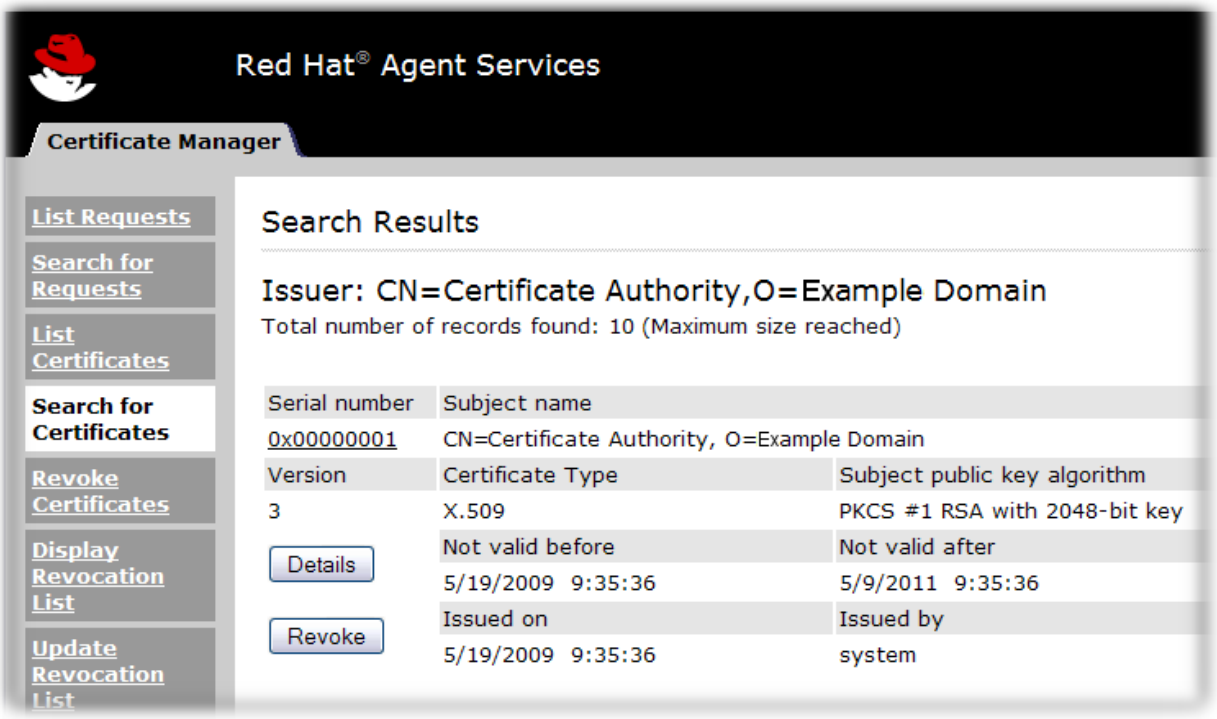


Figure 3.4. Search Results Form

3.3. Approving Requests

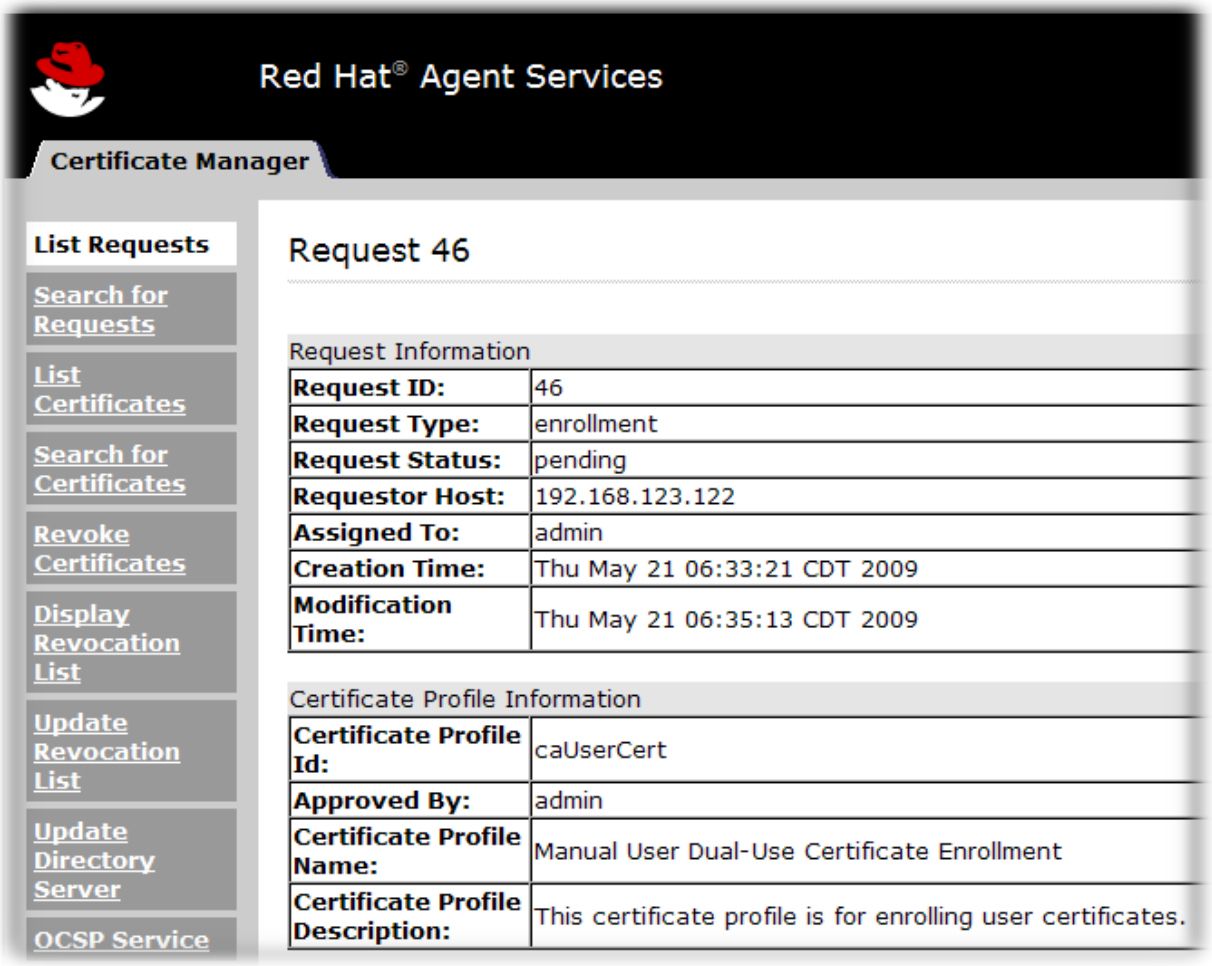
There are two ways that a certificate request is approved, depending on the user authentication method required by the profile. In automatic enrollment, the Certificate System automatically receives and approves the request if it meets established criteria. In manual enrollment, an agent must review and approve the request. Before approving a request, an agent can adjust some of the parameters, such as the subject name and validity period.

To adjust and approve a certificate request:

1. Open the agent services page.

   ```
   https://server.example.com:9443/ca/agent/ca
   ```

2. Click **Find** at the bottom of the **List requests** page to list pending certificate requests.
3. Select the certificate request from the list.
4. The certificate request details page contains several tables with information about the request.



- *Request Information.* Lists basic information about the request.
- *Certificate Profile Information.* Lists the certificate profile being used, along with basic information about that certificate profile.
- *Certificate Profile Inputs.* Lists the inputs contained in the enrollment form for this certificate profile as well as the values set by the requester.
- *Policy Information.* Lists the policies that apply to this certificate profile, including the definition of the policy, the value placed in the certificate by this specific policy, and the constraints placed on this policy.

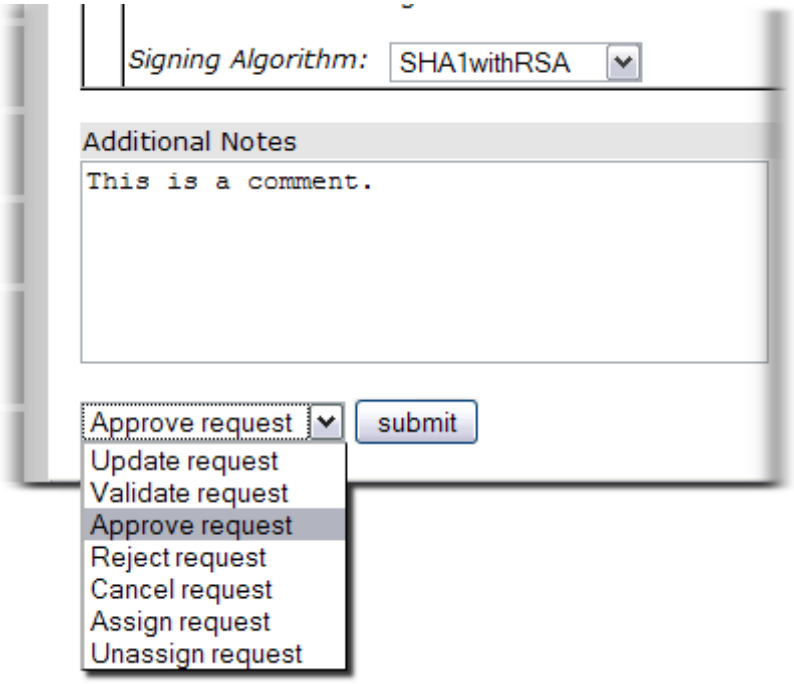
To change any of the information contained in the certificate, such as the subject name or validity period, change the settings in the policy information table in the certificate request. Any policies that can be changed have either a drop-down list or an editable field.

For any changes, the values must be valid within the constraints placed on a policy. If a change is made outside the constraint, the request will not validate. An invalid request must be changed before a certificate is issued.

NOTE

For more information on how to adjust parameters associated with certificate profiles, such as defaults and constraints, see Chapter 2, *CA: Working with Certificate Profiles*.

5. Choose an action from the menu at the bottom of the page, and, optionally, add any comments about the certificate.



- *Approve Request.* Approves the request and issues the certificate.
- *Update Request.* Updates the request with any modified information. The status of the request does not change.
- *Validate Request.* Confirms that the request conforms to the constraints for issuing that type of certificate. The request is confirmed as valid, or the system returns a list of fields that need to be edited.
- *Reject Request.* Rejects the request.
- *Cancel Request.* Cancels the request without issuing a certificate or a rejection.

After the agent sets the action to **`Approve Request`** and clicks **`Submit`**, the certificate is generated and available to the user through the end entities page. If notifications have been set, then an email will be sent to the requester automatically.

3.4. Sending an Issued Certificate to the Requester

When the Certificate Manager has issued a certificate in response to a request, the user who requested it must receive a copy to install locally. Users install user certificates, such as agent certificates, in client software. Server administrators install servers certificates in the servers that they manage.

Depending on how the Certificate System is configured, an end user who requests a certificate might receive automatic email notification of the success of the request; this email message contains either the certificate itself or a URL from which the user can get the certificate.

If the system is not configured for automatic notification or if the requester is a server administrator, the issued certificate must be sent manually to the requester by the agent, or the requester must be directed to retrieve it from the Certificate Manager's end entities page.

Figure 3.5, “A Newly Issued Certificate” shows a web page containing a new certificate. This is the page shown after the agent selects **`Approve this certificate request`**.

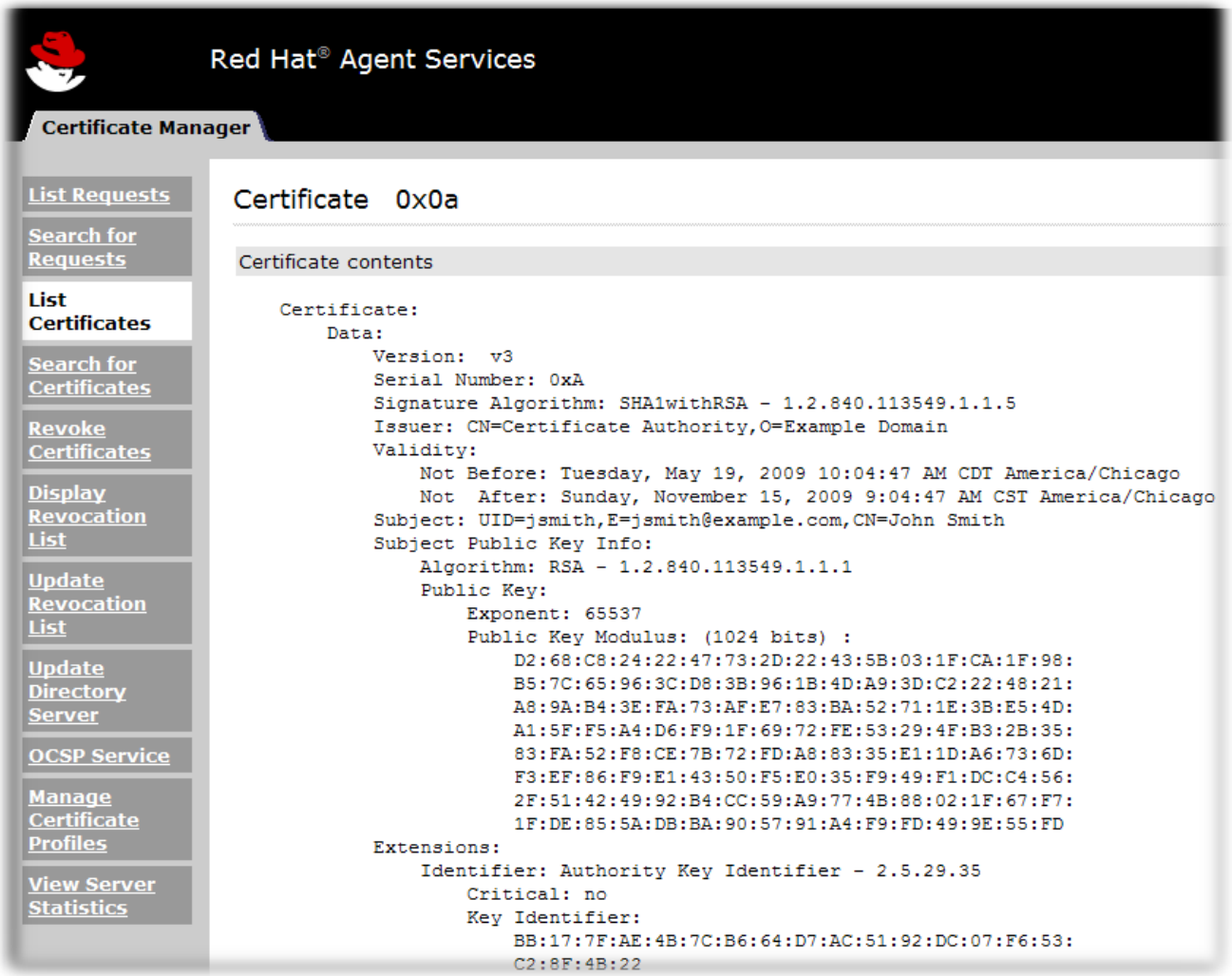


Figure 3.5. A Newly Issued Certificate

To copy and mail a new server certificate to the requester:

TIP

Adminsitrators can configure automatic notifications whenever a certificate is approved so that the requester immediately receives a notification. This is described in chapter 10, "Using Automated Notifications," in the *Certificate System Administrator's Guide*.

1. Create a new email addressed to the requester.
2. Insert in a URL that the requester can use to access the issued certificate. This has the following form:

   ```
   https://hostname:port/ca/ee/ca/displayBySerial?serialNumber=serial_number
   ```

   When the requester follows that link, he only has to click the **Import** button to import the certificate into a browser.

   Alternatively, from the agent services window where the new certificate is displayed, copy only the base-64 encoded certificate, including the marker lines **-----BEGIN CERTIFICATE-----** and **-**

----END CERTIFICATE-----. Paste the base-64 encoded certificate into the email message body, and send the message.

To deliver a new client certificate to the requester, note the serial number of the approved request, and email the number to them. End users can search for and retrieve certificates based on their serial number. If it seems helpful, then include instructions on how to retrieve certificates in the email:

1. Open the end users services page.

   ```
   http://server.example.com:9180/ca/ee/ca
   ```

2. Click the **Retrieval** tab. The **List Certificates** form should appear.
3. Enter the serial number of the certificate in both serial number fields.
4. Click **Find**.
5. When the **Search Results** form appears, click **Details**.
6. When the certificate appears, scroll down to the bottom of the form, and click **Import Certificate**.

Chapter 4. CA: Finding and Revoking Certificates

A Certificate Manager agent can use the agent services page to find a specific certificate issued by the Certificate System or to retrieve a list of certificates that match specified criteria. The certificates which are retrieved can be examined or revoked by the agent. The Certificate Manager agent can also manage the certificate revocation list (CRL).

4.1. Listing Certificates

It is possible to list certificates within a range of serial numbers. All certificates within the range may be displayed or, if the agent selects, only those that are currently valid.

To find a specific certificate or to list certificates by serial number:

1. Open the Certificate Manager agent services page.
2. Click **`List Certificates`**.

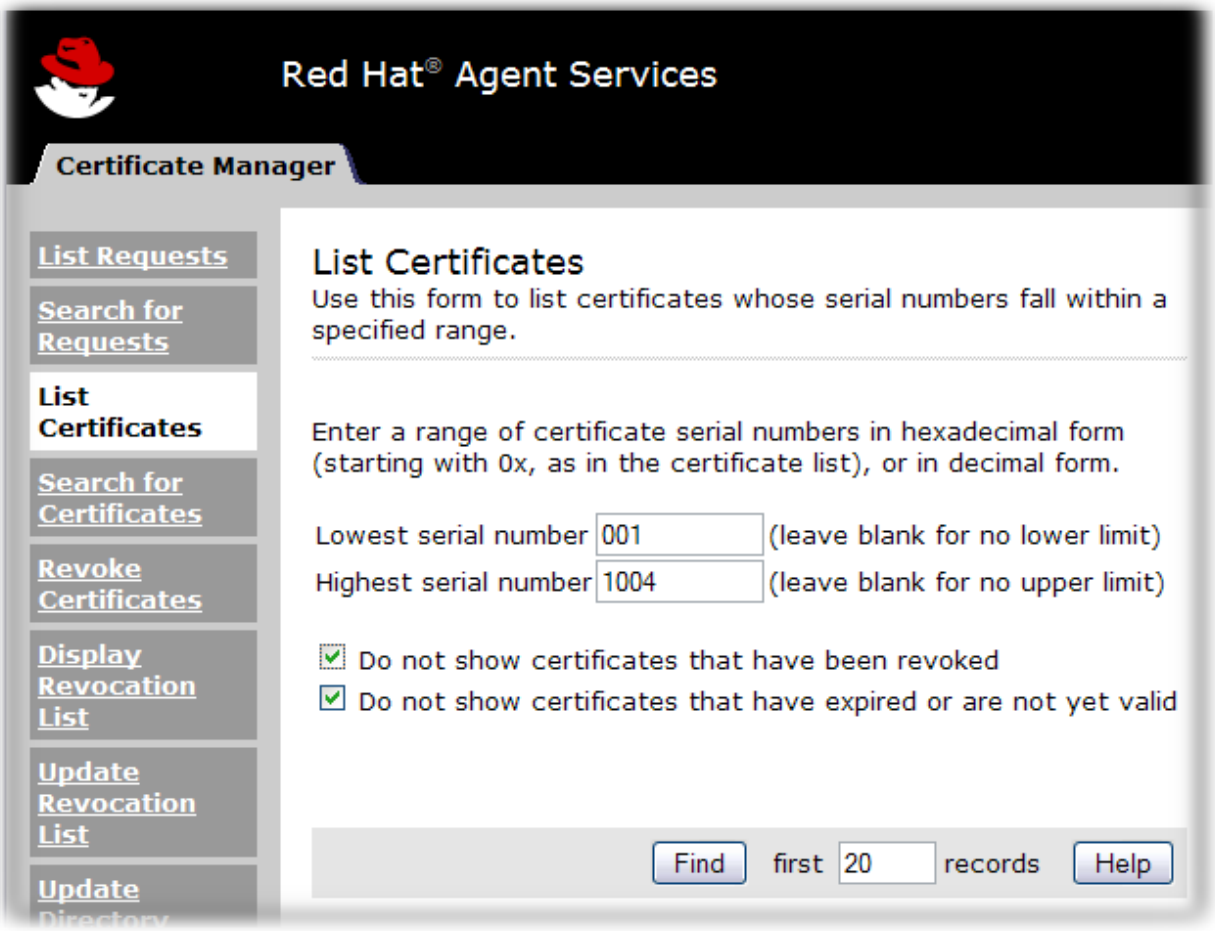

Red Hat® Agent Services
Certificate Manager
List Requests
Search for Requests
List Certificates
Search for Certificates
Revoke Certificates
Display Revocation List
Update Revocation List
Update
List Certificates
Use this form to list certificates whose serial numbers fall within a specified range.
Enter a range of certificate serial numbers in hexadecimal form (starting with 0x, as in the certificate list), or in decimal form.
Lowest serial number 001 (leave blank for no lower limit)
Highest serial number 1004 (leave blank for no upper limit)
Do not show certificates that have been revoked
Do not show certificates that have expired or are not yet valid
Find
first 20 records
Help

Figure 4.1. List Certificates

- To find a certificate with a specific serial number, enter the serial number in both the upper limit and lower limit fields of the **`List Certificates`** form, in either decimal or hexadecimal form. Use **`0x`** to indicate the beginning of a hexadecimal number; for example, **`0x00000006`**. Serial numbers are displayed in hexadecimal form in the **`Search Results`** and **`Details`** pages.
- To find all certificates within a range of serial numbers, enter the upper and lower limits of the serial number range in decimal or hexadecimal form.

Leaving either the lower limit or upper limit field blank displays the certificate with the specified number, plus all certificates before or after it in sequence.

3. To limit the returned list to valid certificates, select the check boxes labeled with filtering methods. It is possible to include revoked certificates, to include expired certificates or certificates that are not yet valid, or to display only valid certificates.
4. Enter the maximum number of certificates matching the criteria that should be returned in the results page.

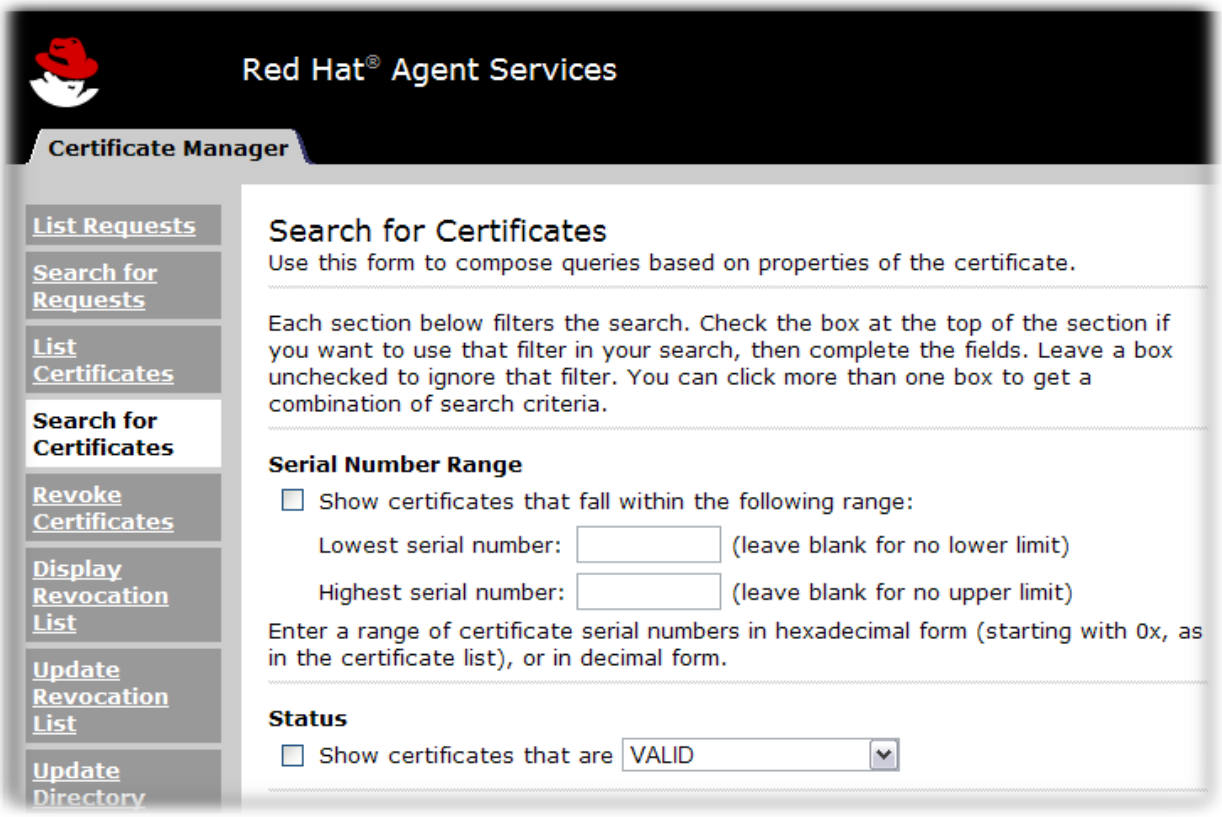
   When any number is entered, the first certificates up to that number matching the criteria are displayed.
5. Click **Find**.

   The Certificate System displays a list of the certificates that match the search criteria. Select a certificate in the list to examine it in more detail or perform various operations on it. For more information, refer to Section 4.3, “Examining Certificate Details”.

4.2. Searching for Certificates (Advanced)

Search for certificates by more complex criteria than serial number using the advanced search form. To perform an advanced search for certificates:

1. Open the Certificate Manager agent services page. The agent must submit the proper client certificate to access this page.
2. Click **Search for Certificates** to display the **Search for Certificates** form to specify search criteria.


Red Hat® Agent Services
Certificate Manager
List Requests
Search for Requests
List Certificates
Search for Certificates
Revoke Certificates
Display Revocation List
Update Revocation List
Update Directory
Search for Certificates
Use this form to compose queries based on properties of the certificate.
Each section below filters the search. Check the box at the top of the section if you want to use that filter in your search, then complete the fields. Leave a box unchecked to ignore that filter. You can click more than one box to get a combination of search criteria.
Serial Number Range
Show certificates that fall within the following range:
Lowest serial number:
(leave blank for no lower limit)
Highest serial number:
(leave blank for no upper limit)
Enter a range of certificate serial numbers in hexadecimal form (starting with 0x, as in the certificate list), or in decimal form.
Status
Show certificates that are
VALID

3. To search by particular criteria, use one or more of the sections of the **Search for Certificates** form. To use a section, select the check box, then fill in any necessary information.
   - *Serial Number Range.* Finds a certificate with a specific serial number or lists all certificates within a range of serial numbers.

- To find a certificate with a specific serial number, enter the serial number in both the upper limit and lower limit fields in either decimal or hexadecimal. Use **0x** to indicate the beginning of a hexadecimal number, such as **0x2A**. Serial numbers are displayed in hexadecimal form in the **Search Results** and **Details** pages.
- To find all certificates within a range of serial numbers, enter the upper and lower limits of the serial number range in decimal or hexadecimal. Leaving either the lower limit or upper limit field blank returns all certificates before or after the number specified.

- *Status.* Selects certificates by their status. A certificate has one of the following status codes:
  - *Valid.* A valid certificate has been issued, its validity period has begun but not ended, and it has not been revoked.
  - *Invalid.* An invalid certificate has been issued, but its validity period has not yet begun.
  - *Revoked.* The certificate has been revoked.
  - *Expired.* An expired certificate has passed the end of its validity period.
  - *Revoked and Expired.* The certificate has passed its validity period and been revoked.
- *Subject Name.* Lists certificates belonging to a particular owner; it is possible to use wildcards in this field.

NOTE

Certificate System certificate request forms support all UTF-8 characters for the common name, organizational unit, and requester name fields. The common name and organization unit fields are included in the subject name of the certificate. This means that the searches for subject names support UTF-8 characters.
This support does not include supporting internationalized domain names.

- *Revocation Information.* Lists certificates that have been revoked during a particular period, by a particular agent, or for a particular reason. For example, an agent can list all certificates revoked between July 2005 and April 2006 or all certificates revoked by the agent with the username **admin**.
  - To list certificates revoked within a time period, select the day, month, and year from the drop-down lists to identify the beginning and end of the period.
  - To list certificates revoked by a particular agent, enter the name of the agent; it is possible to use wildcards in this field.
  - To list certificates revoked for a specific reason, select the revocation reasons from the list.
- *Issuing Information.* Lists certificates that have been issued during a particular period or by a particular agent. For example, an agent can list all certificates issued between July 2005 and April 2006 or all certificates issued by the agent with the username **jsmith**.
  - To list certificates issued within a time period, select the day, month, and year from the drop-down lists to identify the beginning and end of the period.
  - To list certificates issued by a particular agent, enter the name of the agent; it is possible to use wildcards in this field.
  - To list certificates enrolled through a specific profile, enter the name of the profile.
- *Dates of Validity.* List certificates that become effective or expire during a particular period. For example, an agent can list all certificates that became valid on June 1, 2003, or that expired between January 1, 2006, and June 1, 2006.

  It is also possible to list certificates that have a validity period of a certain length of time, such as all certificates that are valid for less than one month.
  - To list certificates that become effective or expire within a time period, select the day,

month, and year from the drop-down lists to identify the beginning and end of the period.

- To list certificates that have a validity period of a certain length in time, select **Not greater than** or **Not less than** from the drop-down list, enter a number, and select a time unit from the drop-down list: days, weeks, months, or years.

- *Basic Constraints.* Shows CA certificates that are based on the Basic Constraints extension.
- *Type.* Lists certain types of certificates, such as all certificates for subordinate CAs. This search works only for certificates containing the Netscape Certificate Type extension, which stores type information. For each type, choose from the drop-down list to find certificates where that type is **On**, **Off**, or **Do Not Care**.

4. To find a certificate with a specific subject name, use the **Subject Name** section. Select the check box, then enter the subject name criteria. Enter values for the included search criteria and leave the others blank.

   The standard tags or components are as follows:

   - *Email address.* Narrows the search by email address.
   - *Common name.* Finds certificates associated with a specific person or server.
   - *UserID.* Searches certificates by the user ID for the person to whom the certificate belongs.
   - *Organization unit.* Narrows the search to a specific division, department, or unit within an organization.
   - *Organization.* Narrows the search by organization.
   - *Locality.* Narrows the search by locality, such as the city.
   - *State.* Narrows the search by state or province.
   - *Country.* Narrows the search by country; use the two-letter country code, such as **US**.

   NOTE

   Certificate System certificate request forms support all UTF-8 characters for the common name and organizational unit fields. The common name and organization unit fields are included in the subject name of the certificate. This means that the searches for subject names or those elements in the subject name support UTF-8 characters.
   This support does not include supporting internationalized domain names, such as in email addresses.

5. After entering the field values for the server to match, specify the type of search to perform:

   - Exact searches for certificate subject names match the exact components specified and contain none of the components left blank. Wildcards cannot be used in this type of search.
   - Partial searches for certificate subject names match the specified components, but the returned certificates may also contain values in components that were left blank. Wildcard patterns can be used in this type of search by using a question mark (**?**) to match an arbitrary single character and an asterisk (*****) to match an arbitrary string of characters.

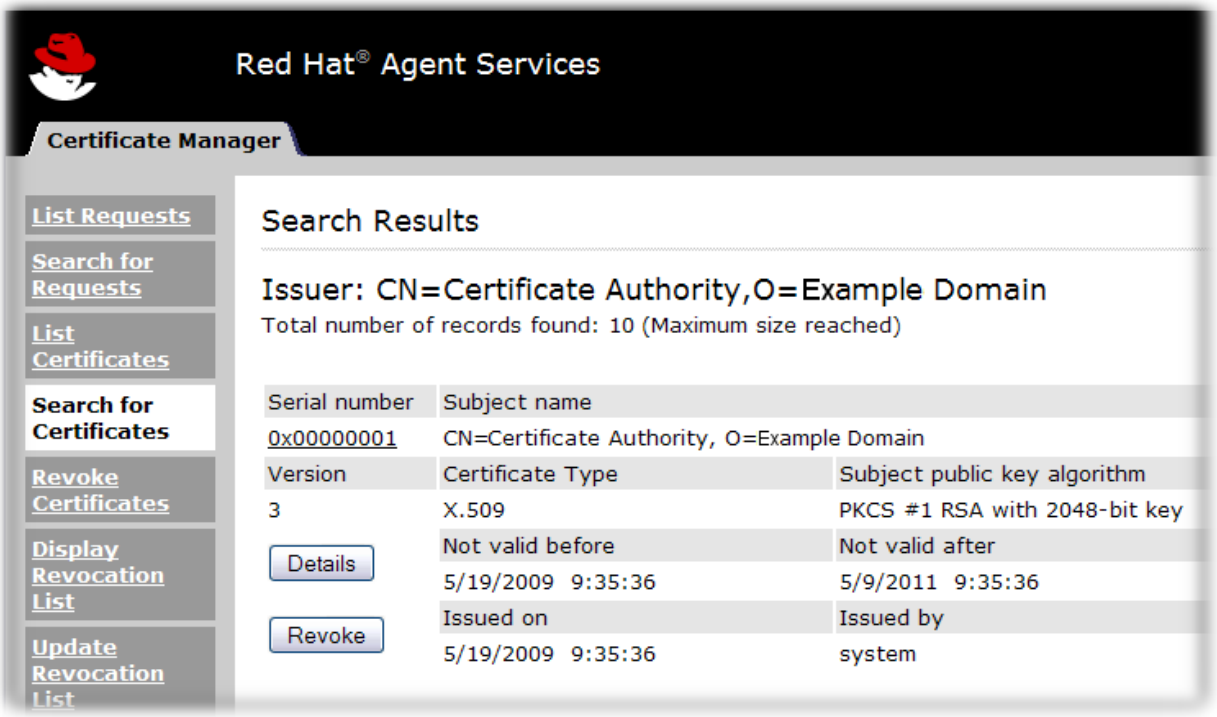
     NOTE

     Placing a single asterisk in a search field means that the component must be in the certificate's subject name but may have any value. Leave the field blank if it does not matter if the field is present.

6. After entering the search criteria, scroll to the bottom of the form, and enter the number of certificates matching the specified criteria that should be returned.

Setting the number of certificates to be returned returns the first certificates found that match the search criteria up to that number. It is also possible to put a time limit on the search in seconds.

7. Click **Find**.
8. The **Search Results** form appears, showing a list of the certificates that match the search criteria. Select a certificate in the list to examine it in more detail. For more information, refer to Section 4.3, “Examining Certificate Details”.



4.3. Examining Certificate Details

1. On the agent services page, click **List Certificates** or **Search for Certificates**, specify search criteria, and click **Find** to display a list of certificates.
2. On the **Search Results** form, select a certificate to examine.

   If the desired certificate is not shown, scroll to the bottom of the list, specify an additional number of certificates to be returned, and click **Find**. The system displays the next certificates up to that number that match the original search criteria.
3. After selecting a certificate, click the **Details** button at the left side of its entry.
4. The **Certificate** page shows the detailed contents of the selected certificate and instructions for installing the certificate in a server or in a web browser.

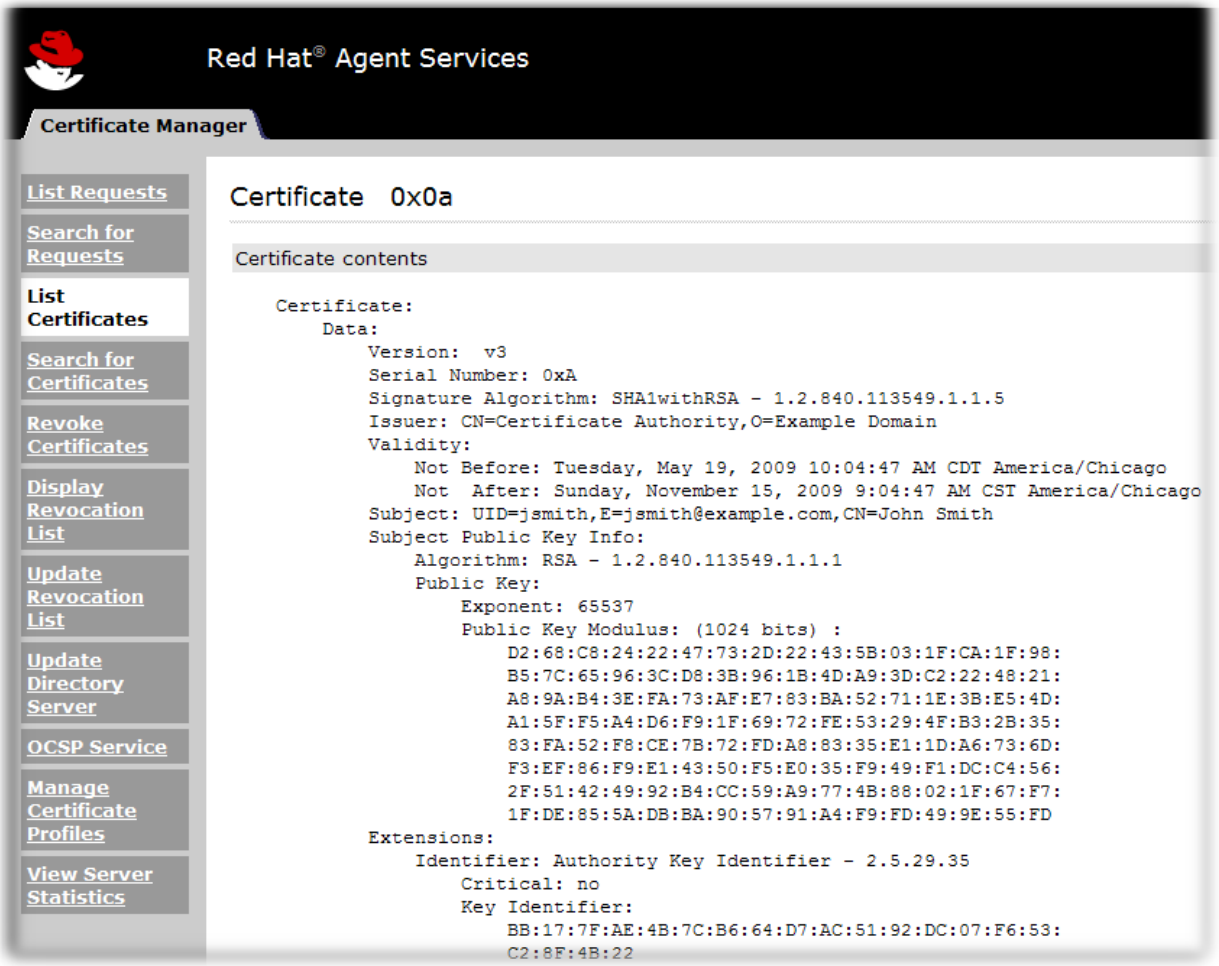


Figure 4.2. Certificate Details

5. The certificate is shown in base-64 encoded form at the bottom of the **Certificate** page, under the heading **Installing this certificate in a server**.

4.4. Revoking Certificates

Only Certificate Manager agents can revoke certificates other than their own. A certificate must be revoked if one of the following situations occurs:

- The owner of the certificate has changed status and no longer has the right to use the certificate.
- The private key of a certificate owner has been compromised.

These two reasons are not the only ones why a certificate would need revoked; there are six reasons available for revoking a certificate.

To revoke one or more certificates, search for the certificates to revoke using the **Revoke Certificates** button. While the search is similar to the one through the **Search for Certificates** form, the **Search Results** form returned by this search offers the option of revoking one or all of the returned certificates.

4.4.1. Revoking Certificates

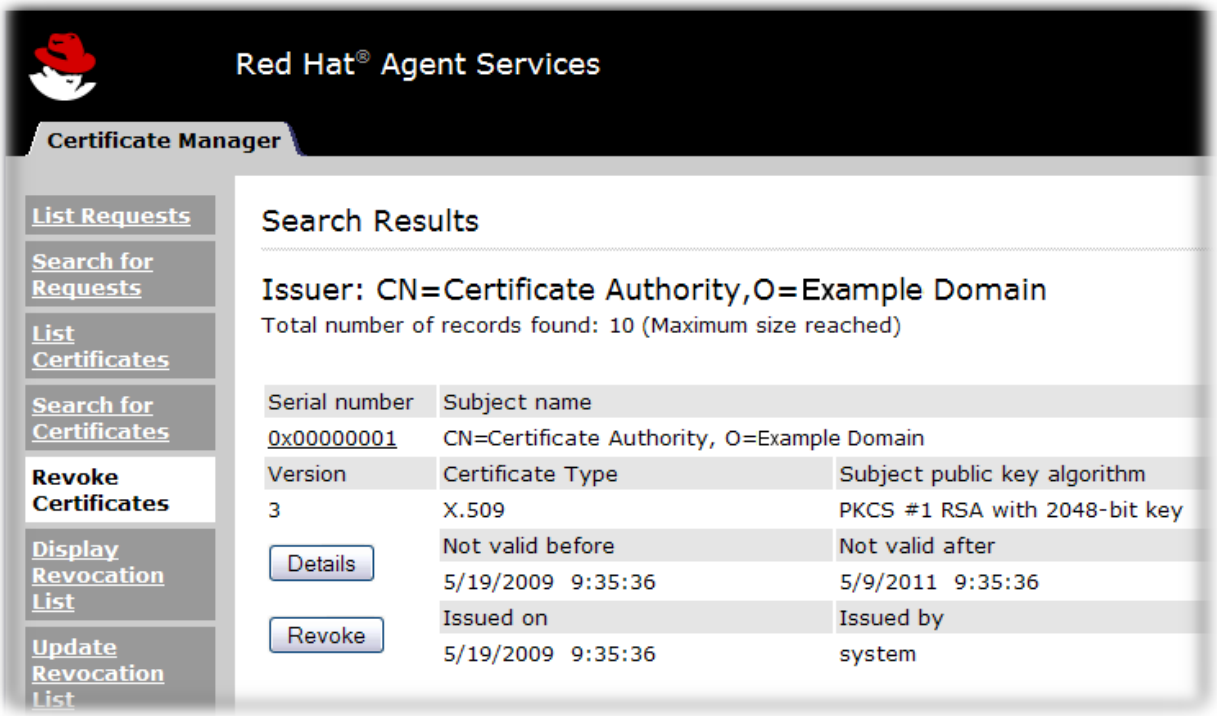
1. Open the Certificate Manager agent services page.

2. Click **Revoke Certificates**.

NOTE

The search form that appears has the same search criteria sections as the **Search for Certificates** form.

3. Specify the search criteria by selecting the check boxes for the sections and filling in the required information.
4. Scroll to the bottom of the form, and set the number of matching certificates to display.
5. Click **Find**.
6. The search returns a list of matching certificates. It is possible to revoke one or all certificates in the list.



TIP

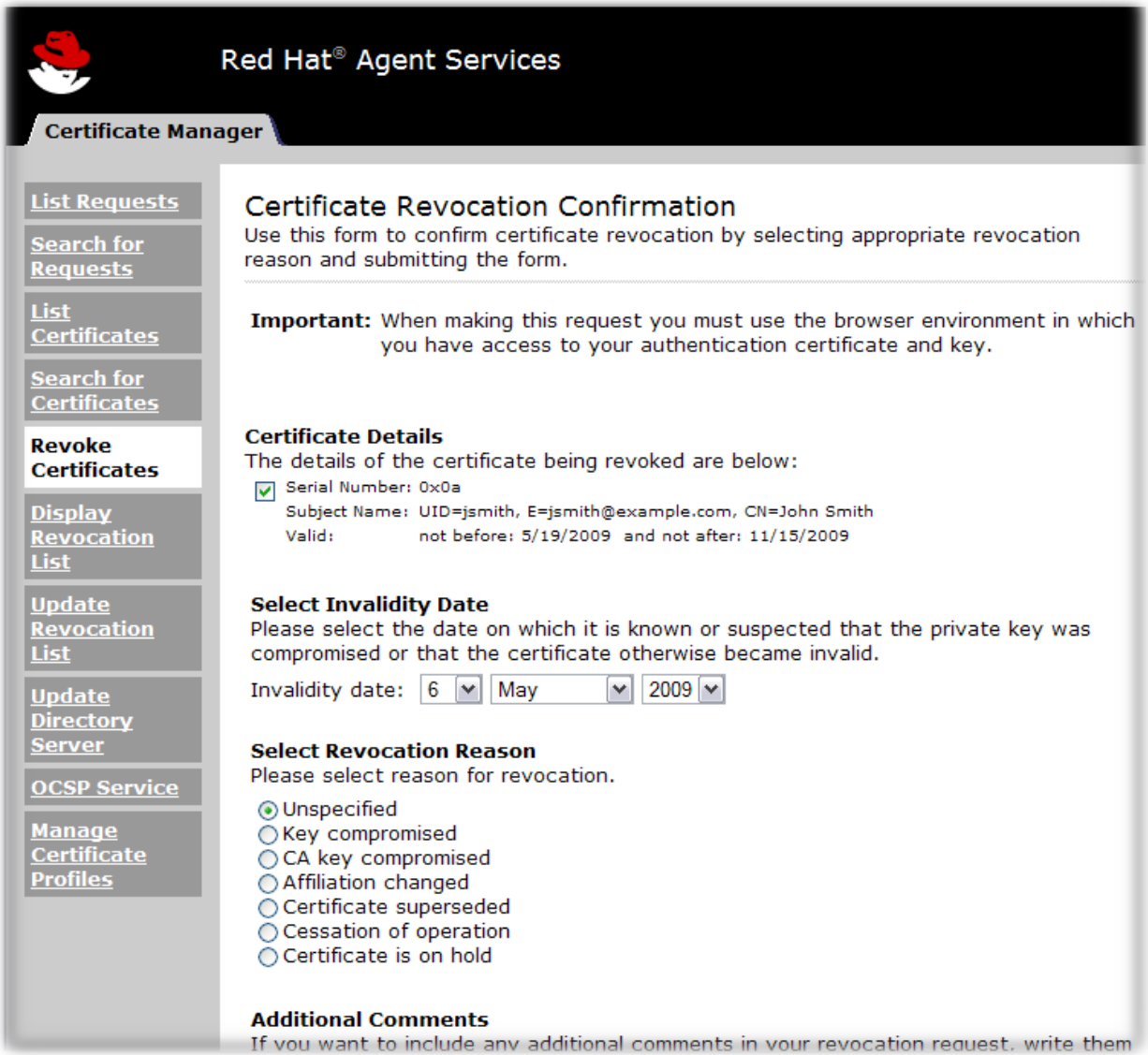
If the search criteria are very specific and all of the certificates returned are to be revoked, then click the **Revoke ALL # Certificates** button at the bottom of the page. The number shown on the button is the total number of certificates returned by the search. This is usually a larger number than the number of certificates displayed on the current page. Verify that all of the certificates returned by the search should be revoked, *not* only those displayed on the current page.

7. Click the **Revoke** button next to the certificate to be revoked.

CAUTION

Whether revoking a single certificate or a list of certificates, be extremely careful that the correct certificate has been selected or that the list contains only certificates which should be revoked. Once a revocation operation has been confirmed, there is no way to undo it.

8. Select an invalidity date. The invalidity date is the date which it is known or suspected that the user's private key was compromised or that the certificate became invalid. A set of drop down lists allows the agent to select the correct invalidity date.


Red Hat® Agent Services
Certificate Manager
List Requests
Search for Requests
List Certificates
Search for Certificates
Revoke Certificates
Display Revocation List
Update Revocation List
Update Directory Server
OCSP Service
Manage Certificate Profiles
Certificate Revocation Confirmation
Use this form to confirm certificate revocation by selecting appropriate revocation reason and submitting the form.
Important: When making this request you must use the browser environment in which you have access to your authentication certificate and key.
Certificate Details
The details of the certificate being revoked are below:
Serial Number: 0x0a
Subject Name: UID=jsmith, E=jsmith@example.com, CN=John Smith
Valid: not before: 5/19/2009 and not after: 11/15/2009
Select Invalidity Date
Please select the date on which it is known or suspected that the private key was compromised or that the certificate otherwise became invalid.
Invalidity date: 6 May 2009
Select Revocation Reason
Please select reason for revocation.
Unspecified
Key compromised
CA key compromised
Affiliation changed
Certificate superseded
Cessation of operation
Certificate is on hold
Additional Comments

9. Select a reason for the revocation.
   - Key compromised
   - CA key compromised
   - Affiliation changed
   - Certificate superseded
   - Cessation of operation
   - Certificate is on hold
10. Enter any additional comment. The comment is included in the revocation request.

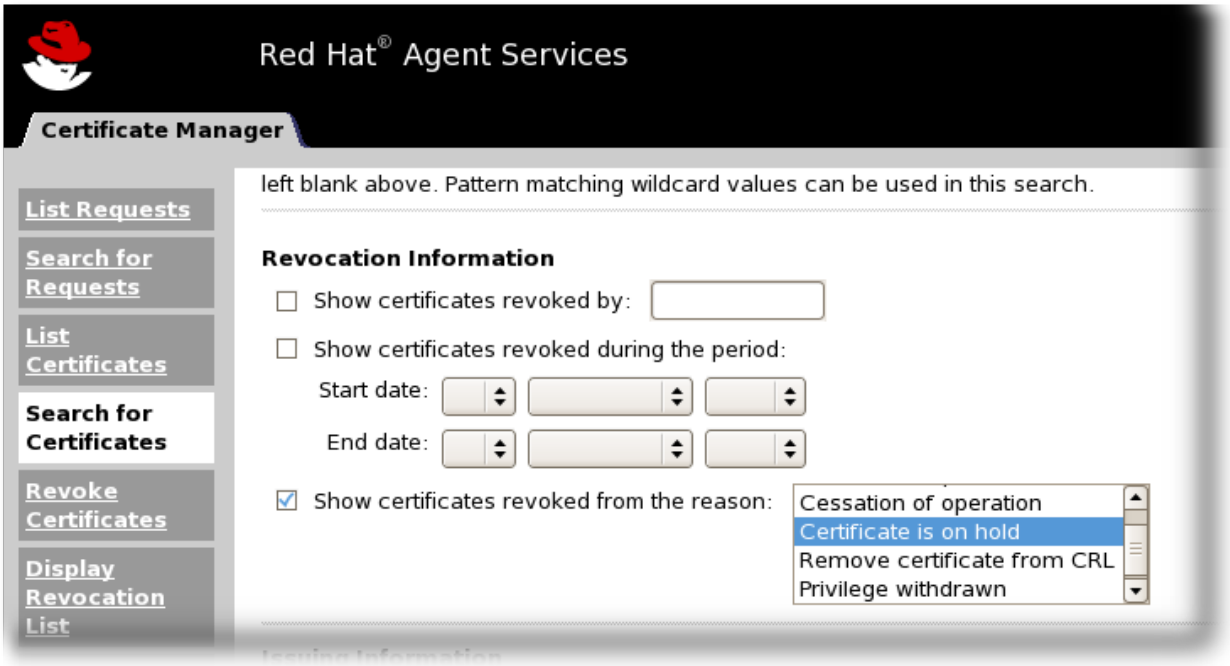
When the revocation request is submitted, it is automatically approved, and the certificate is revoked. Revocation requests are viewed by listing requests with a status of **Completed**; see Section 3.2, "Listing Certificate Requests" for more information.

4.4.2. Taking Ceritificates Off Hold

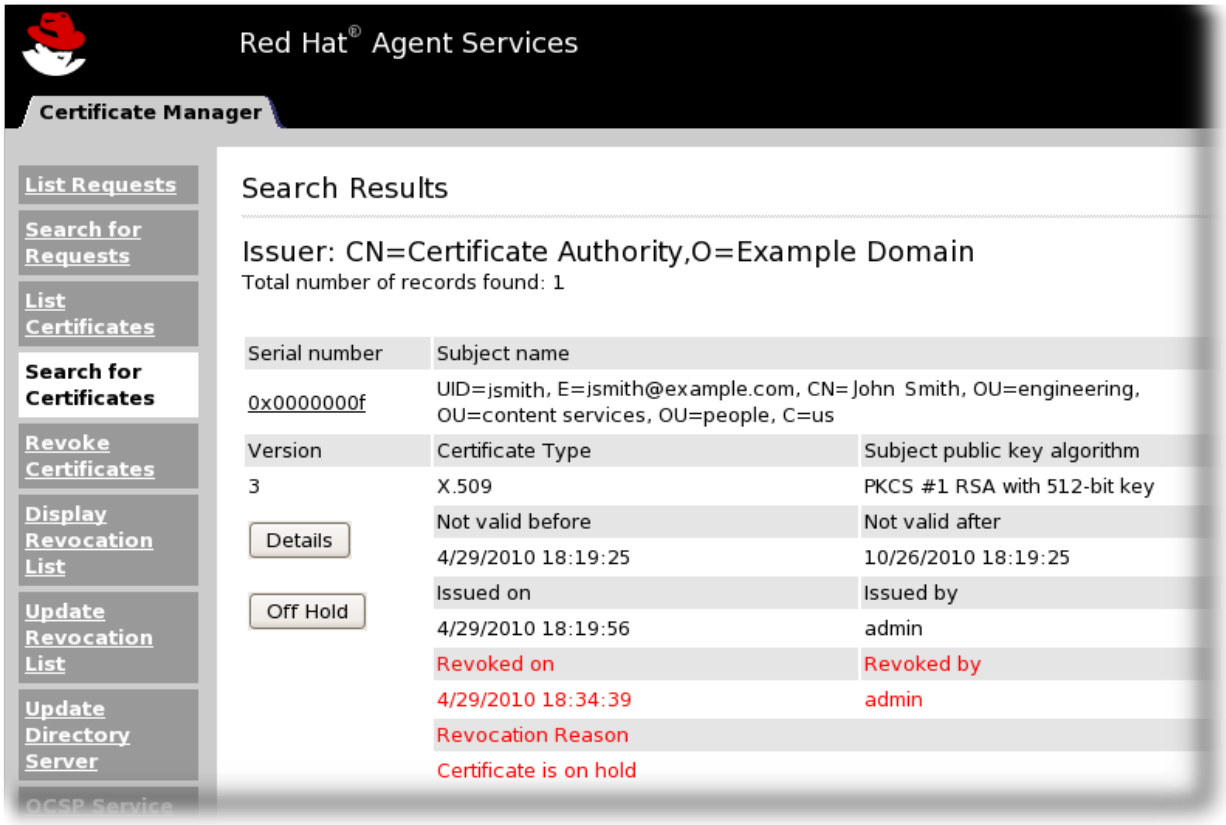
There can be instances when a certificate is inaccessible, and therefore should be treated as revoked, but that certificate can be recovered. For example, a user may have a personal email certificate stored on a flash drive which he accidentally leaves at home. The certificate is not compromised, but it should be temporarily suspended.

That certificate can be temporarily revoked by putting it on hold (one of the options given when revoking a certificate, as in Section 4.4.1, "Revoking Certificates"). At a later time — such as when the forgotten flash drive is picked up — that certificate can be taken off hold and is again active.

1. Search for the on hold certificate, as in Section 4.2, "Searching for Certificates (Advanced)". Scroll to the **Revocation Information** section, and set the **Certificate is on hold** revocation reason as the search criterion.



2. In the results list, click the **Off Hold** button by the certificate to take off hold.



4.5. Managing the Certificate Revocation List

Revoking a certificate notifies other users that the certificate is no longer valid. This notification is done by publishing a list of the revoked certificates, called the *certificate revocation list* (CRL), to an LDAP directory or to a flat file. This list is publicly available and ensures that revoked certificates are not misused.

4.5.1. Viewing or Examining CRLs

It may be necessary to view or examine a CRL, such as before manually updating a directory with the latest CRL. To view or display the CRL:

1. Go to the Certificate Manager agent services page.
2. Click **`Display Certificate Revocation List`** to display the form for viewing the CRL.
3. Select the CRL to view. If the administrator has created multiple issuing points, these are listed in the **Issuing point** drop-down list. Otherwise, only the master CRL is shown.
4. Choose how to display the CRL by selecting one of the options from the **Display Type** menu. The choices on this menu are as follows:
   - *Cached CRL.* Views the CRL from the cache rather than from the CRL itself. This option displays results faster than viewing the entire CRL.
   - *Entire CRL.* Retrieves and displays the entire CRL.
   - *CRL header.* Retrieves and displays the CRL header only.
   - *Base 64 Encoded.* Retrieves and displays the CRL in base-64 encoded format.
   - *Delta CRL.* Retrieves and displays a delta CRL, which is a subset of the CRL showing only new revocations since the last CRL was published. This option is available only if delta CRL generation is enabled.
5. To examine the selected CRL, click **`Display`**.

The CRL appears in the browser window. This allows the agent to check whether a particular certificate (by its serial number) appears in the list and to note recent changes such as the total number of certificates revoked since the last update, the total number of certificates taken off hold since the last update, and the total number of certificates that expired since the last update.

4.5.2. Updating the CRL

CRLs can be automatically updated if a schedule for automatic CRL generation is enabled, and the schedule can set the CRL to be generated at set time schedules or whenever there are certificate revocations.

Likewise, CRLs can be also automatically published if CRL publishing is enabled.

In some cases, the CRL may need to be updated manually, such as updating the list after the system has been down or removing expired certificates to reduce the file size. (Expired certificates do not need to be included in the CRL because they are already invalid because of the expiration date.) Only a Certificate Manager agent can manually update the CRL.

To update the CRL manually:

1. Open the Certificate Manager agent services page.
2. Click **`Update Revocation List`** to display the form for updating the CRL.

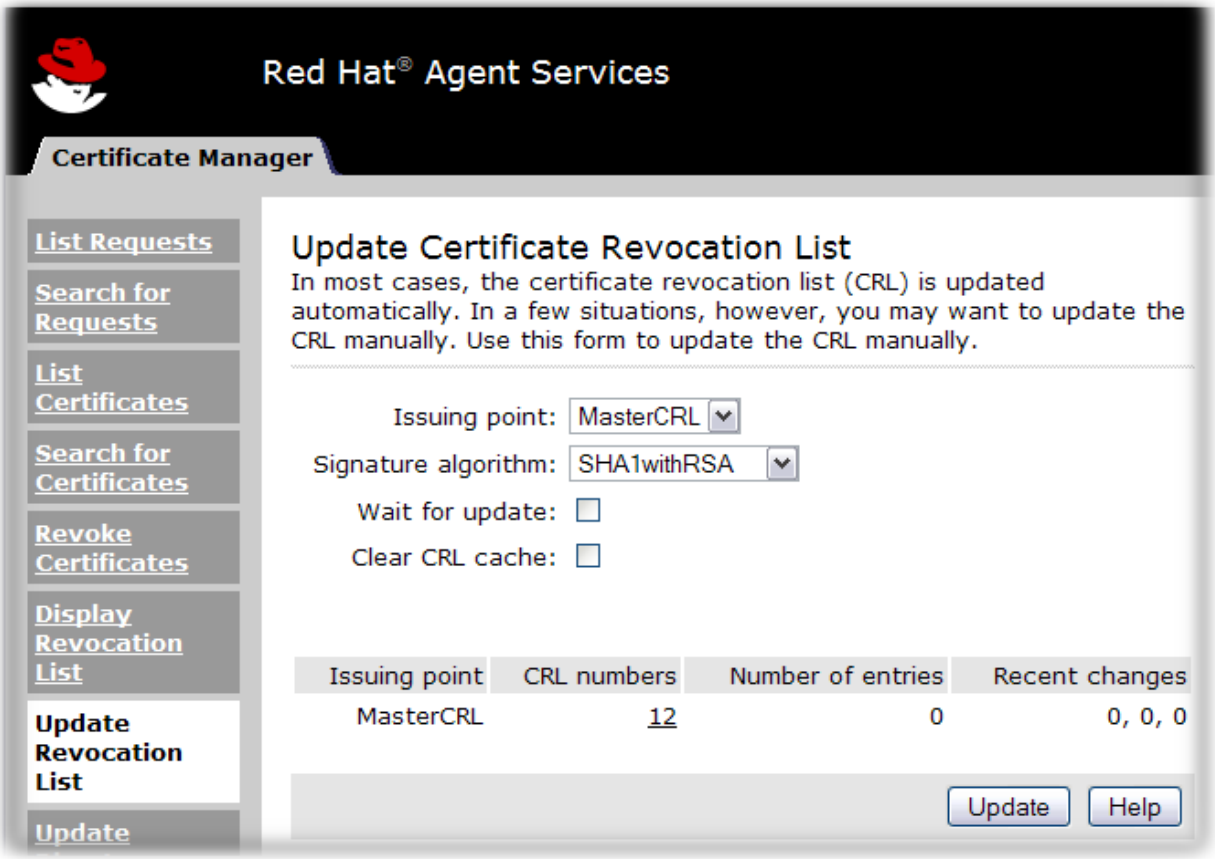


Figure 4.3. Update Certificate Revocation List

3. Select the CRL issuing point which will update the CRL. There can be multiple issuing points configured for a single CA.
4. Select the algorithm to use to sign the new CRL. Before choosing an algorithm, make sure that any system or network applications that need to read or view this CRL support the algorithm.

- SHA-1 with RSA generates a 160-bit message digest.
- SHA-256 with RSA.
- SHA-512 with RSA.
- MD5 with RSA generates a 128-bit message digest. Most existing software applications that handle certificates support only MD5. This is the default algorithm.
- MD2 with RSA generates a 128-bit message digest.

Before selecting an algorithm, make sure that the Certificate System has that algorithm enabled. The Certificate System administrator will have that information.

5. Click **Update** to update the CRL with the latest certificate revocation information.

Chapter 5. CA: Publishing to a Directory

A Red Hat Directory Server installation is required for the Certificate System subsystems to be installed; this directory instance maintains user information and certificate and key information. The Certificate System can be configured to publish certificates and CRLs to that directory, or other LDAP directories, for other applications to access. Certificate information published to the publishing directory must be periodically updated as certificates are issued and revoked. Updates are usually published automatically but may also be published manually.

This chapter describes the procedures for updating an LDAP directory with the current status of certificates. Only a Certificate Manager agent can manage publishing certificates and CRLs to the directory.

5.1. Automatically Updating the Directory

Once the Certificate System administrator has configured the Certificate System to publish to the publishing Directory Server, any changes to certificate information in Certificate System are automatically updated in the publishing directory at specific times.

- The first time the Certificate System is started, it publishes the Certificate Manager's CA certificate to the LDAP publishing directory.
- When the Certificate System issues a new certificate, the certificate is published to the LDAP publishing directory.
- When the Certificate System revokes a certificate, the certificate is removed from the publishing directory.
- When the CRL is created or updated, the list is published to the LDAP publishing directory.

For more information on configuring the Certificate System to publish to the Directory Server, see the *Certificate System Administrator's Guide*.

5.2. Manually Updating the Directory

The LDAP publishing directory usually does not need certificate data updated manually because most updates are automatic. However, it may be necessary to update the LDAP publishing directory manually in the following situations:

- The publishing Directory Server is down for a period of time and unable to receive changes from the Certificate System.
- Expired certificates need to be removed from the publishing directory since certificates are not automatically removed from the publishing directory when they expire.

NOTE

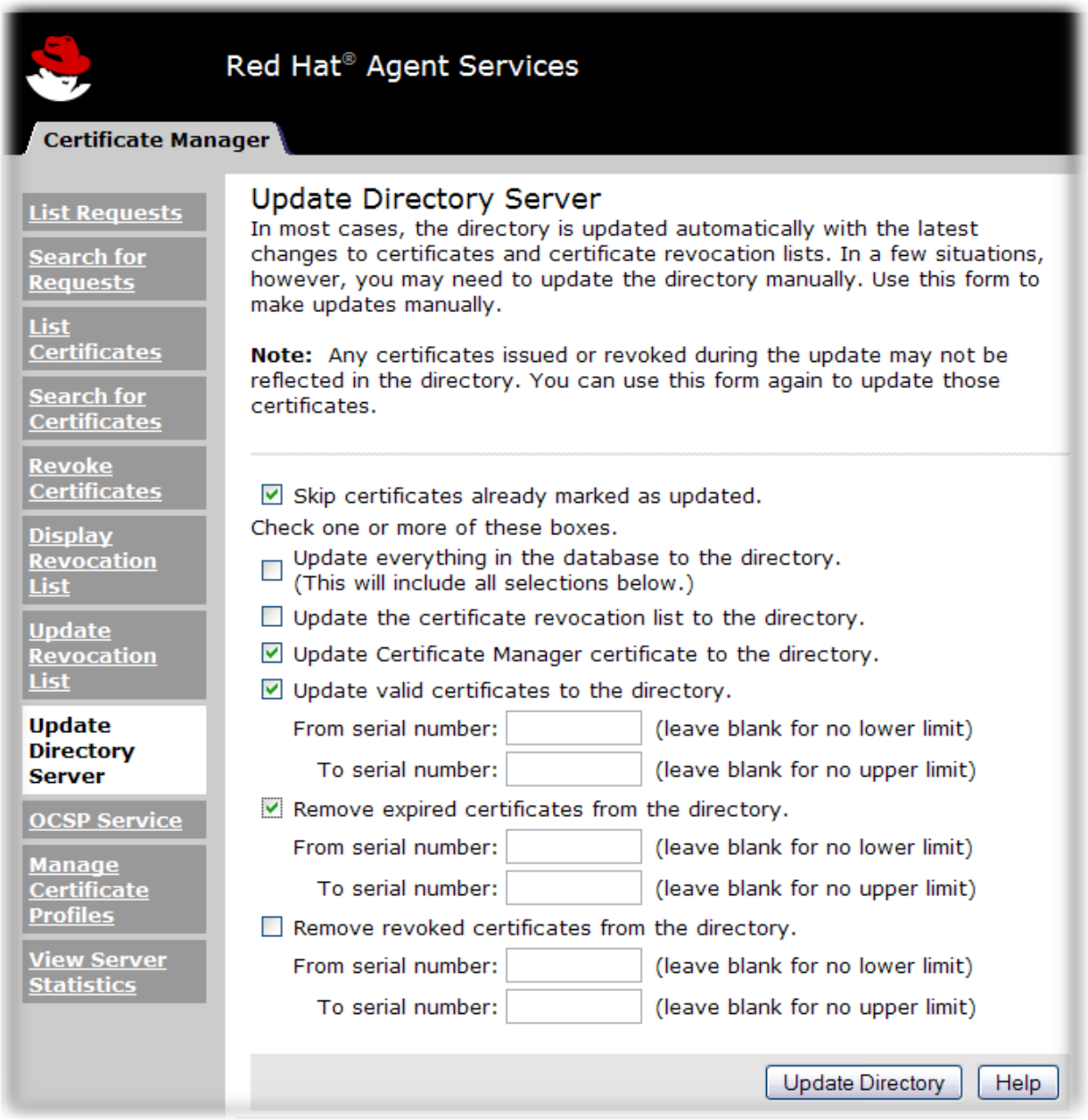
Any client using a certificate is responsible for determining its validity by checking the expiration date against the client's current date information.

To update the LDAP publishing directory with changes manually:

1. Open the Certificate Manager agent services page.

```
https://server.example.com:9443/ca/agent/ca
```

2. Click **`Update Directory Server`** to open the publishing page.


Red Hat® Agent Services
Certificate Manager
List Requests
Search for Requests
List Certificates
Search for Certificates
Revoke Certificates
Display Revocation List
Update Revocation List
Update Directory Server
OCSP Service
Manage Certificate Profiles
View Server Statistics
Update Directory Server
In most cases, the directory is updated automatically with the latest changes to certificates and certificate revocation lists. In a few situations, however, you may need to update the directory manually. Use this form to make updates manually.
Note: Any certificates issued or revoked during the update may not be reflected in the directory. You can use this form again to update those certificates.
Skip certificates already marked as updated.
Check one or more of these boxes.
Update everything in the database to the directory. (This will include all selections below.)
Update the certificate revocation list to the directory.
Update Certificate Manager certificate to the directory.
Update valid certificates to the directory.
From serial number: (leave blank for no lower limit)
To serial number: (leave blank for no upper limit)
Remove expired certificates from the directory.
From serial number: (leave blank for no lower limit)
To serial number: (leave blank for no upper limit)
Remove revoked certificates from the directory.
From serial number: (leave blank for no lower limit)
To serial number: (leave blank for no upper limit)
Update Directory
Help

3. Select **`Skip certificates already marked as updated`** to ignore certificates in the internal database that have already been published or removed, in the case of revoked certificates.

   In some circumstances, updating the LDAP publishing directory can take considerable time. During this period, any changes made through the Certificate System such as issuing or revoking certificates may not be included in the update. If certificates have been issued or revoked during that time, the publishing directory must be updated again to reflect those changes. Use the **`Skip certificates already marked as updated`** option the second time to update only certificates that been issued, revoked, or expired while the previous update was running.

4. Select the type of update to perform.
   - To publish the latest CRL, select **`Update the certificate revocation list to the publishing directory`**.
   - To update information on valid certificates to the publishing directory, select **`Update valid certificates to the directory`**.

     To update a range of certificates, such as only the most recently issued certificates, specify

the range of the serial numbers of those certificates.

- To remove expired certificates from the publishing directory, select **Remove expired certificates from the directory**.

  To remove a range of certificates instead of all expired certificates, specify the range of the serial numbers of those certificates.

- To remove revoked certificates from the publishing directory, select **Remove revoked certificates from the directory**.

  If you want to remove a range of certificates instead of all revoked certificates, specify the range of the serial numbers of those certificates.

5. After specifying the changes to be updated, click **Update Directory**.

Chapter 6. RA: Requesting and Receiving Certificates Locally

The Registration Authority (RA) subsystem allows certificates to be requested and approved *locally*. Locally can encompass any kind of division: different departments, geographical locations, or employee types. The purpose of a Registration Manager is to bring the approval process for certificates to a grassroots level, where people who actually know or are responsible for a requester are capable of assessing their certificate requests.

Using a Registration Manager relieves the load on centralized CAs.

The RAs have more limited options than CAs, concentrating on certificates for users, servers, and routers. The requests are approved by the RA agent and are then issued by the CA.

6.1. Listing Certificate Requests

Listing requests initially returns all certificate requests submitted or generated through the RA instance. These can be filtered by their status (open, approved, rejected, or failed).

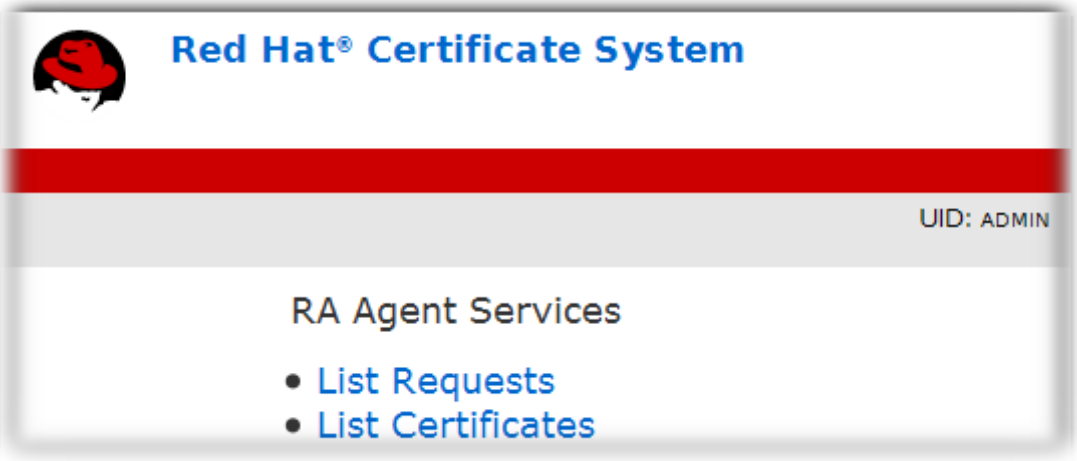
NOTE

Open requests have not yet been processed by an RA agent, while rejected requests were rejected by the RA agent. Approved and failed both mean that the initial request was approved by the RA agent, and have been processed by the CA, one successfully (approved) and one unsuccessfully (failed).

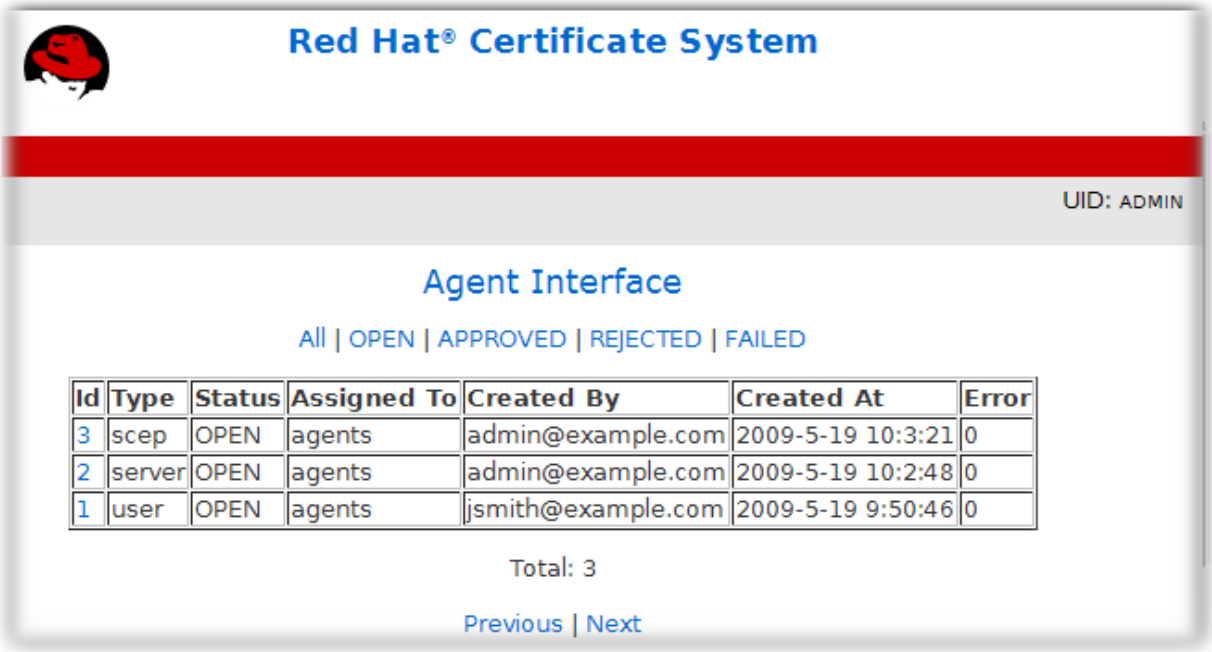
1. Open the RA agent services page.

```
https://server.example.com:12889/agent/index.cgi
```

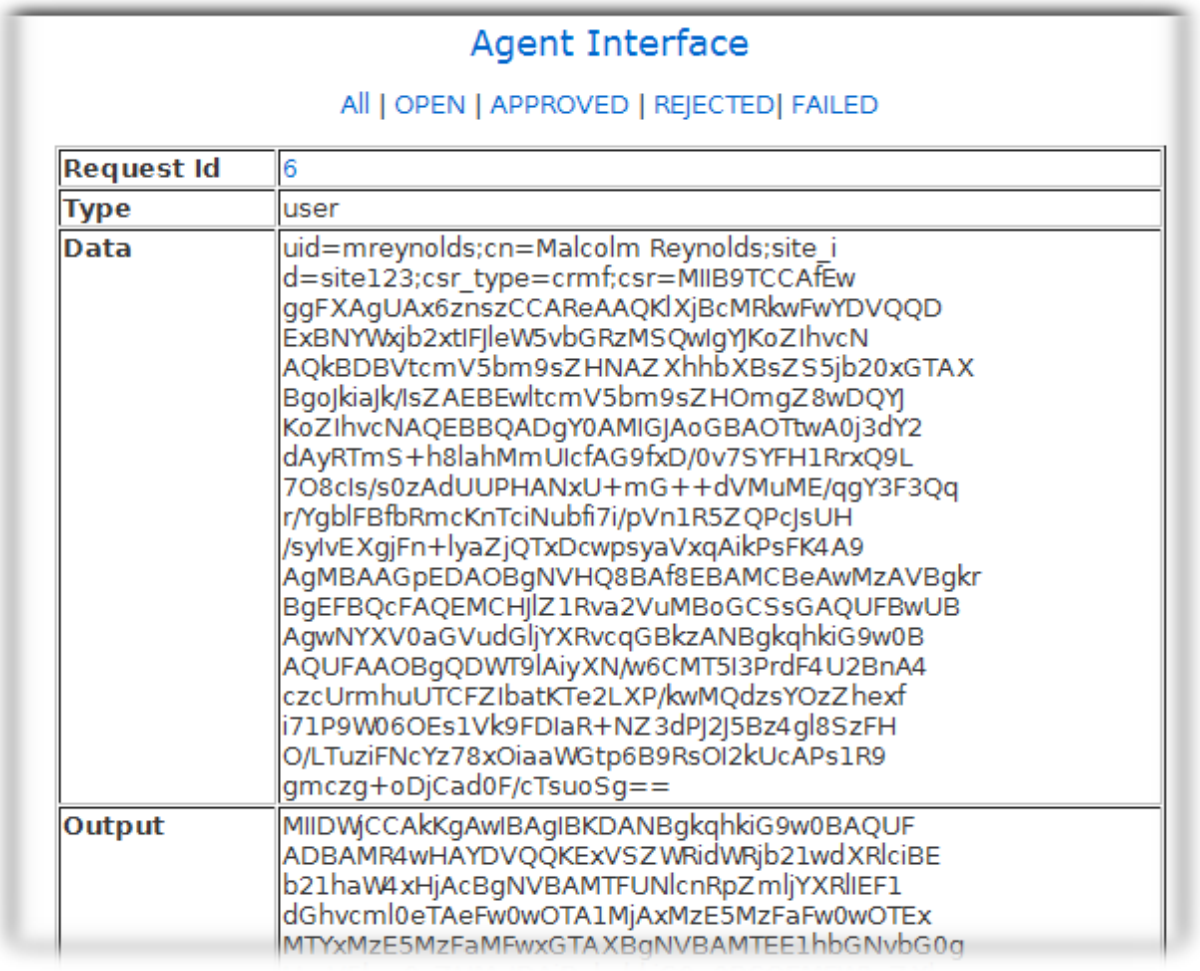
2. Click the **`List Requests`** link.



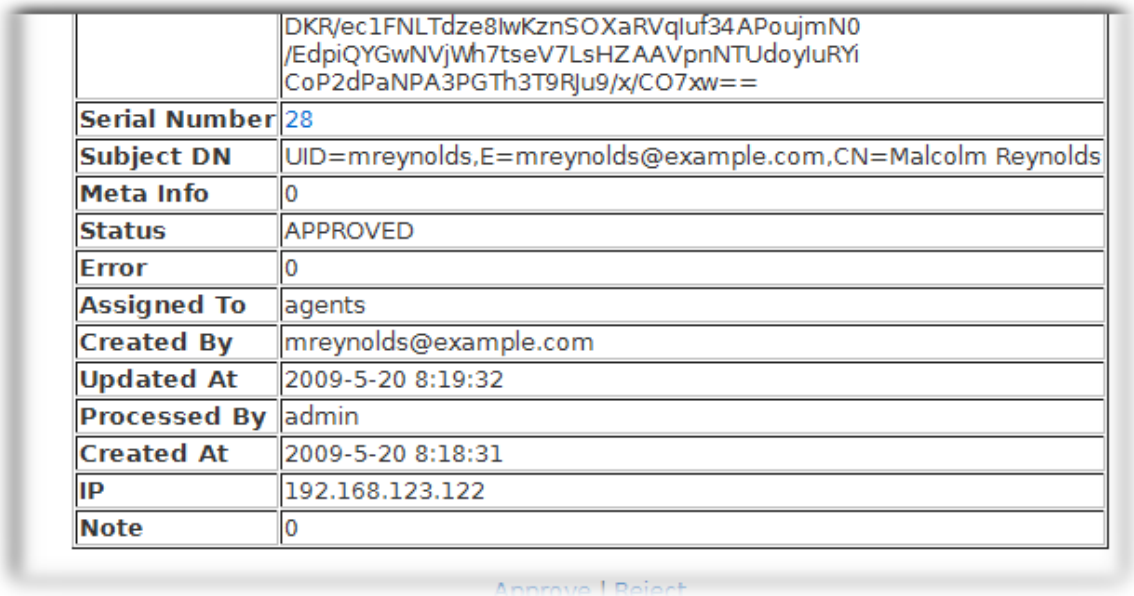
3. All of the requests which have been submitted or generated through the RA are listed.


Red Hat® Certificate System
UID: ADMIN
Agent Interface
All | OPEN | APPROVED | REJECTED | FAILED
Id Type Status Assigned To Created By Created At Error
3 scep OPEN agents admin@example.com 2009-5-19 10:3:21 0
2 server OPEN agents admin@example.com 2009-5-19 10:2:48 0
1 user OPEN agents jsmith@example.com 2009-5-19 9:50:46 0
Total: 3
Previous | Next

4. Click the **`Request ID`** for the request to view it.
5. The top part of the request details contains the data used for the request and the base-64 encoded blob of the certificate request.



The bottom half of the details page shows information like notes for the request, the time it was submitted and, if it has been processed, the time and agent who reviewed it.



	DKR/ec1FNLTdze8IwKznSOXaRVqIuf34APoujmN0 /EdpiQYGwNVjWh7tseV7LsHZAAVpnNTUdoyIuRYi CoP2dPaNPA3PGTh3T9RJu9/x/CO7xw==
Serial Number	28
Subject DN	UID=mreynolds,E=mreynolds@example.com,CN=Malcolm Reynolds
Meta Info	0
Status	APPROVED
Error	0
Assigned To	agents
Created By	mreynolds@example.com
Updated At	2009-5-20 8:19:32
Processed By	admin
Created At	2009-5-20 8:18:31
IP	192.168.123.122
Note	0

Approve | Reject

6.2. Approving Certificate Requests

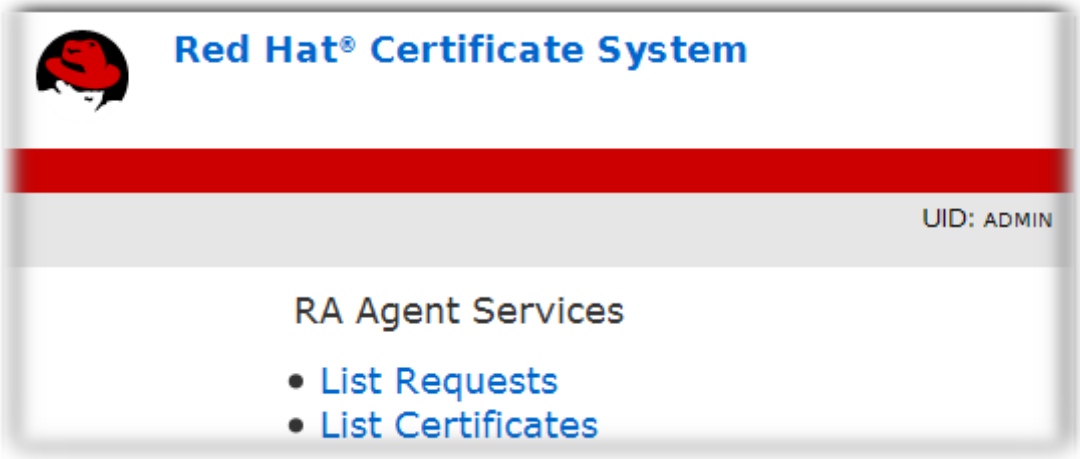
After the certificate request has been received, it needs to be approved by the RA agent. Approved requests are immediately sent to the CA to be issued.

To approve the certificate request:

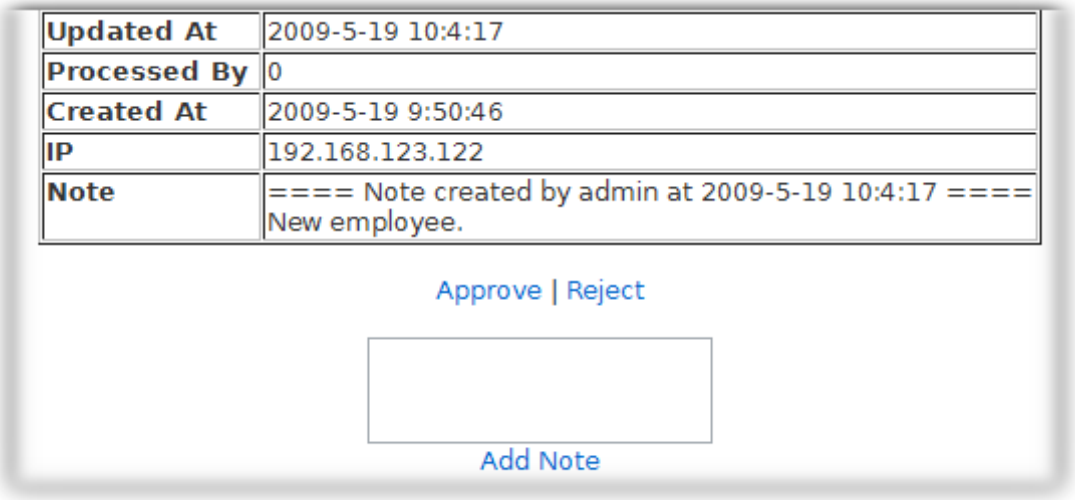
1. Open the RA agent services page.

   ```
   https://server.example.com:12889/agent/index.cgi
   ```

2. Click the **`List Requests`** link.



3. Scroll to the bottom of the screen and add an optional note to the certificate request, and click **`Add Note`**.
4. Click **`Approve`** to approve the request.



Once the request is approved, the method for delivering the approved certificate varies. For example, for RA agent requests, the CA immediately returns a PIN to use to claim the approved certificate. Other users may be able to access their certificate request in the end-entities page and retrieve the certificate immediately.

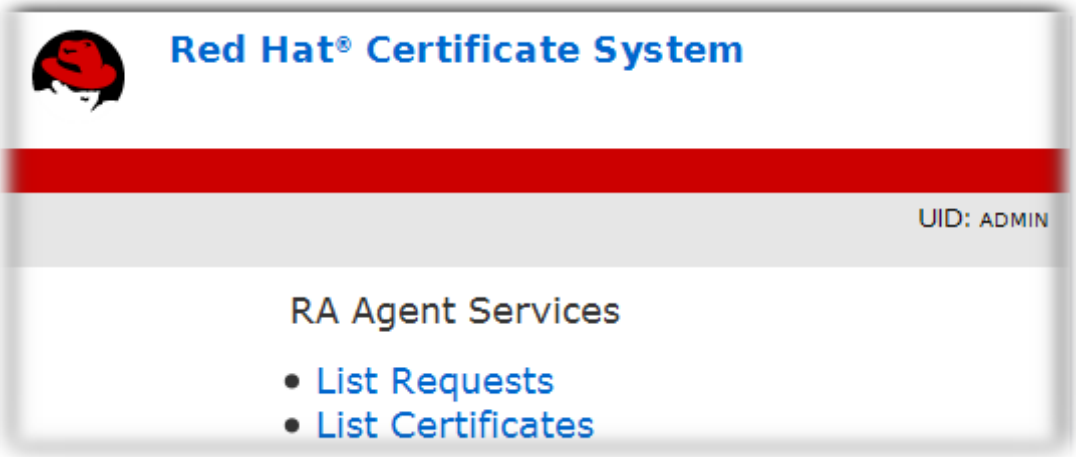
6.3. Listing Certificates

Unlike the CA, which can filter and search for specific certificates issued, the only way to find a certificate processed through the RA is to list all certificates.

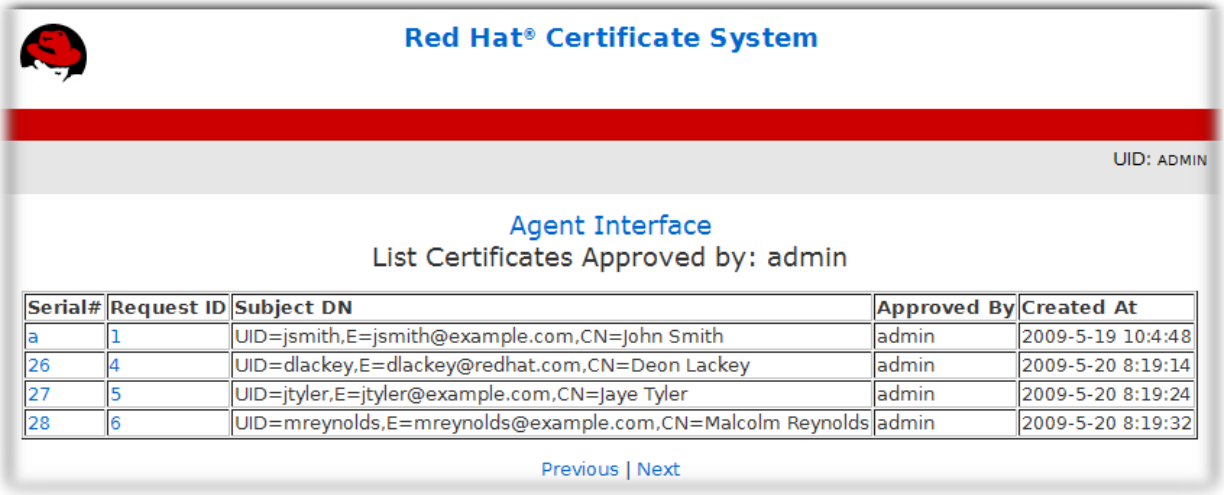
1. Open the RA agent services page.

   ```
   https://server.example.com:12889/agent/index.cgi
   ```

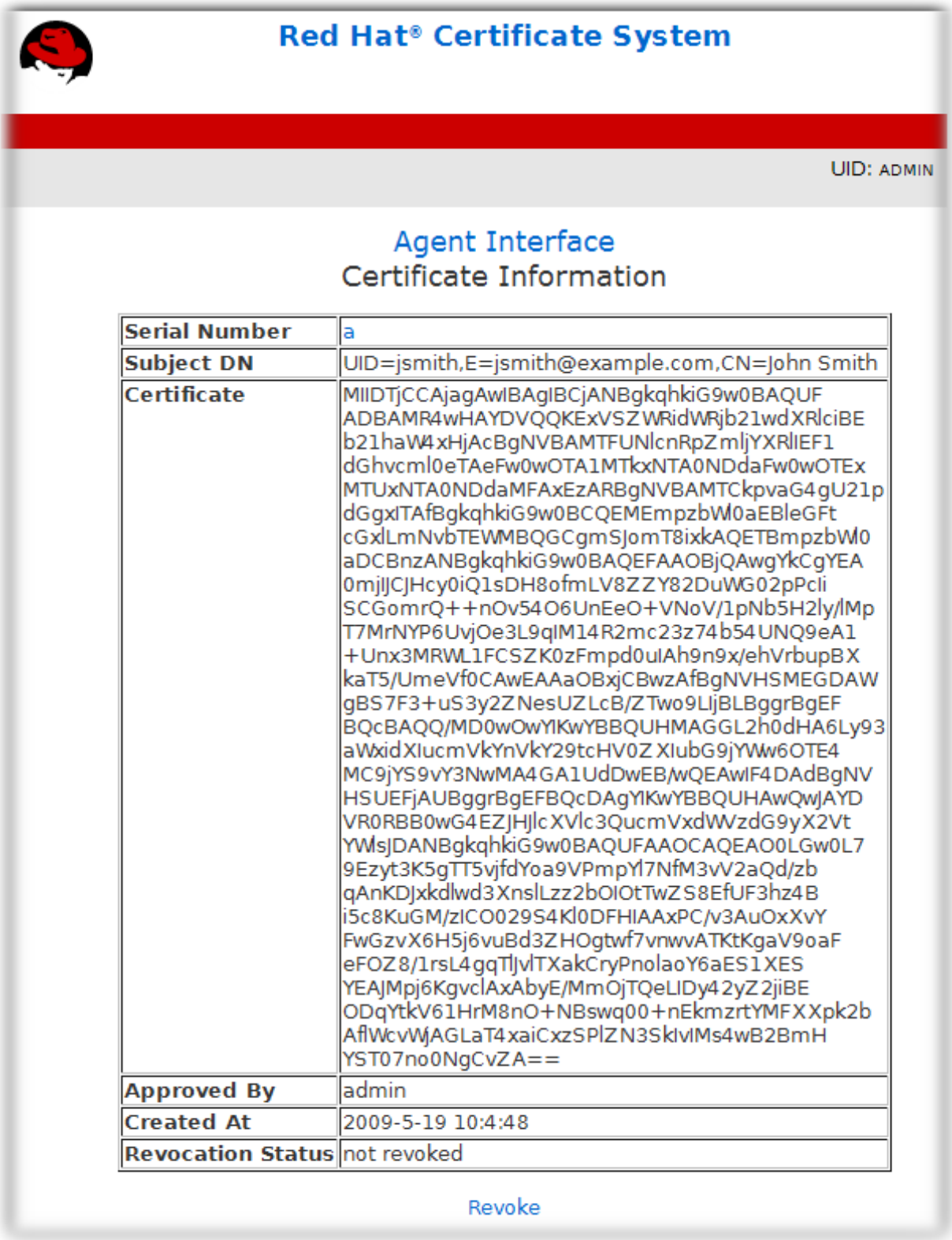
2. Click the **`List Certificates`** link.



3. All of the certificates which have been processed through the RA are listed.


Red Hat® Certificate System
UID: ADMIN
Agent Interface
List Certificates Approved by: admin
Serial# Request ID Subject DN Approved By Created At
a 1 UID=jsmith,E=jsmith@example.com,CN=John Smith admin 2009-5-19 10:4:48
26 4 UID=dlackey,E=dlackey@redhat.com,CN=Deon Lackey admin 2009-5-20 8:19:14
27 5 UID=jtyler,E=jtyler@example.com,CN=Jaye Tyler admin 2009-5-20 8:19:24
28 6 UID=mreynolds,E=mreynolds@example.com,CN=Malcolm Reynolds admin 2009-5-20 8:19:32
Previous | Next

4. To view the certificate, click the **Serial#** list for it. To see the original certificate request, then click the **Request ID** for it.



Red Hat® Certificate System

UID: ADMIN

Agent Interface

Certificate Information

Serial Number	a
Subject DN	UID=jsmith,E=jsmith@example.com,CN=John Smith
Certificate	MIIDTjCCAjagAwIBAgIBCjANBgkqhkiG9w0BAQUF ADBAMR4wHAYDVQQKExVSZWRidWRjb21wdXRlciBE b21haW4xHjAcBgNVBAMTFUNlcnRpZmljYXRlIEF1 dGhvcml0eTAeFw0wOTA1MTkxNTA0NDdaFw0wOTEx MTUxNTA0NDdaMFAxEzARBgNVBAMTCkpvaG4gU21p dGgxITAfBgkqhkiG9w0BCQEMEmpzbWl0aEBleGFt cGxlLmNvbTEWMBQGCgmSJomT8ixkAQETBmpzbWl0 aDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA 0mjIJCJHcy0iQ1sDH8ofmLV8ZZY82DuWG02pPcIi SCGomrQ++nOv54O6UnEeO+VNoV/1pNb5H2ly/lMp T7MrNYP6UvjOe3L9qIM14R2mc23z74b54UNQ9eA1 +Unx3MRWL1FCSZK0zFmpd0uIAh9n9x/ehVrbupBX kaT5/UmeVf0CAwEAAaOBxjCBwzAfBgNVHSMEGDAW gBS7F3+uS3y2ZNesUZLcB/ZTwo9LIjBLBggrBgEF BQcBAQQ/MD0wOwYIKwYBBQUHMAGGL2h0dHA6Ly93 aWxidXIucmVkYnVkY29tcHV0ZXIubG9jYWw6OTE4 MC9jYS9vY3NwMA4GA1UdDwEB/wQEAwIF4DAdBgNV HSUEFjAUBggrBgEFBQcDAgYIKwYBBQUHAwQwJAYD VR0RBB0wG4EZJHJlcXVlc3QucmVxdWVzdG9yX2Vt YWlsJDANBgkqhkiG9w0BAQUFAAOCAQEAO0LGw0L7 9Ezyt3K5gTT5vjfdYoa9VPmpYl7NfM3vV2aQd/zb qAnKDJxkdlwd3XnslLzz2bOIOtTwZS8EfUF3hz4B i5c8KuGM/zICO029S4Kl0DFHIAAxPC/v3AuOxXvY FwGzvX6H5j6vuBd3ZHOgtwf7vnwvATKtKgaV9oaF eFOZ8/1rsL4gqTlJvlTXakCryPnolaoY6aES1XES YEAJMpj6KgvclAxAbyE/MmOjTQeLIDy42yZ2jiBE ODqYtkV61HrM8nO+NBswq00+nEkmzrtYMFXXpk2b AflWcvWjAGLaT4xaiCxzSPlZN3SkIvIMs4wB2BmH YST07no0NgCvZA==
Approved By	admin
Created At	2009-5-19 10:4:48
Revocation Status	not revoked

Revoke

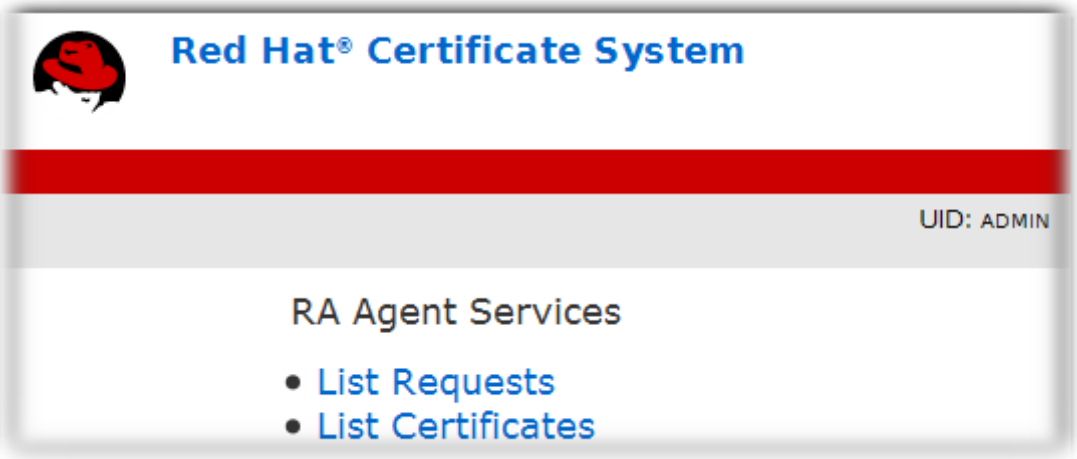
6.4. Revoking Certificates

RA agents can revoke certificates that were approved through that Registration Manager instance.

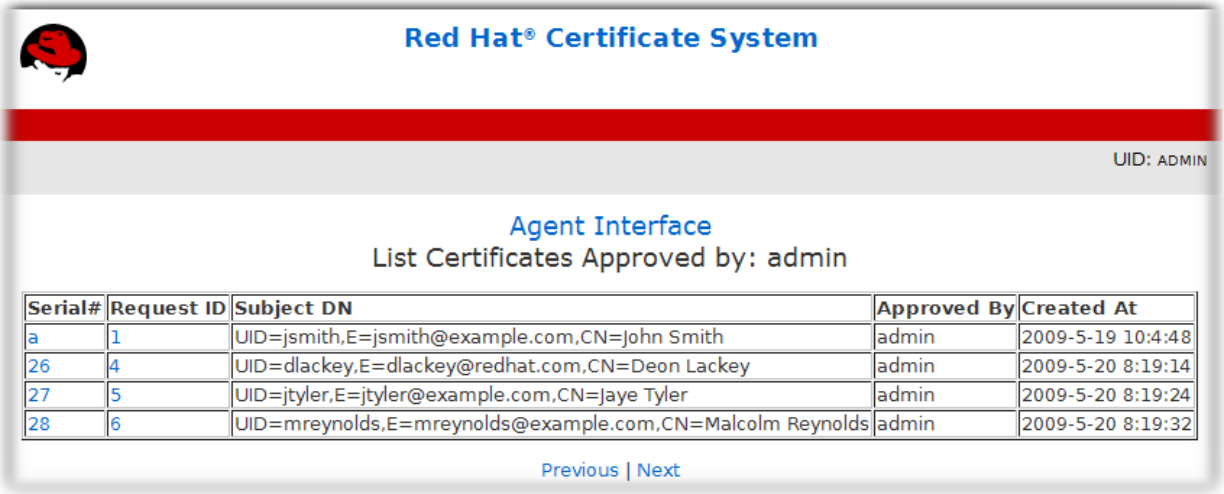
1. Open the RA agent services page.

```
https://server.example.com:12889/agent/index.cgi
```

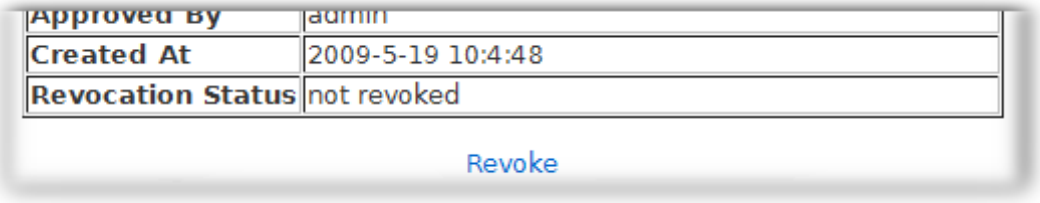
2. Click the **List Certificates** link.



3. All of the certificates which have been processed through the RA are listed.


Red Hat® Certificate System
UID: ADMIN
Agent Interface
List Certificates Approved by: admin
Serial# Request ID Subject DN Approved By Created At
a 1 UID=jsmith,E=jsmith@example.com,CN=John Smith admin 2009-5-19 10:4:48
26 4 UID=dlackey,E=dlackey@redhat.com,CN=Deon Lackey admin 2009-5-20 8:19:14
27 5 UID=jtyler,E=jtyler@example.com,CN=Jaye Tyler admin 2009-5-20 8:19:24
28 6 UID=mreynolds,E=mreynolds@example.com,CN=Malcolm Reynolds admin 2009-5-20 8:19:32
Previous | Next

4. Open the certificate to revoke by clicking its **Serial#** in the certificate list.
5. At the bottom of the certificate's details page, click the **Revoke** link.



6. Select the reason that the certificate is being revoked, and then confirm the revocation.

6.5. Creating and Managing Users and Groups for an RA

When an RA is first created, certain default users and groups with default roles are created automatically. An initial user, **admin**, is created with both agent and administrator roles, and two groups are created to identify agent and administrator users. Additional users and additional groups can be added to manage the RA subsystem and PKI operations.

The RA uses web-based services pages to services page for the RA, so, like the TPS, administrative tasks like managing users and groups are carried out through the RA web services pages.

There is a division between agent tasks and administrative tasks, even though both sets of functions are accessed through web services pages. RA agent tasks manage operations related to issuing

certificates, like approving requests. RA administrator tasks relate to managing the server instance, mainly managing users and groups.

6.5.1. Managing RA Groups

By default, the RA has administrator and agent groups. Other groups can be configured, depending on the local demands of the PKI and network, and then the new group can be assigned to function as an administrative or agent group.

A user can perform tasks based on what groups he is a member of. An RA agent, for example, must belong to the RA group to perform agent tasks.

6.5.1.1. Listing Groups for an RA

1. Open the RA services page.

   ```
   https://server.example.com:12889/services
   ```

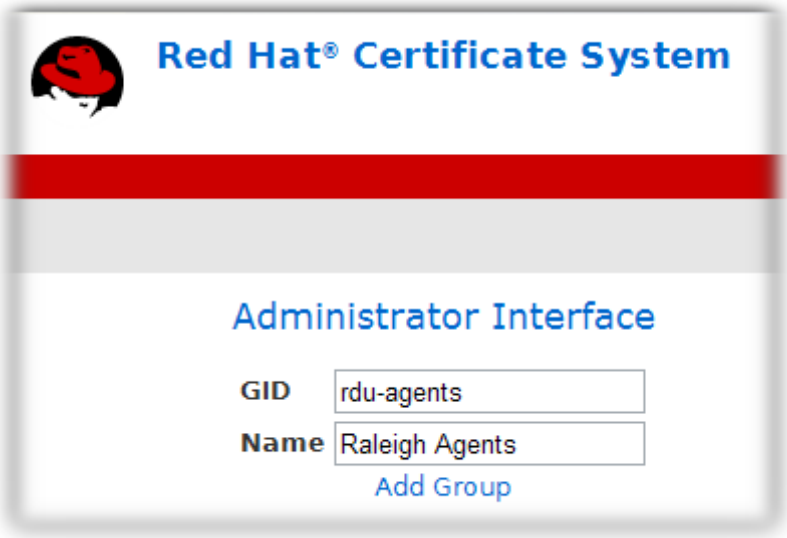
2. Click the **Administrator Services** link.
3. Click the **List Groups** link.
4. There are two default groups, for agents and for administrators. To view the details about any group, click the GID of the group.

6.5.1.2. Creating a New Group for an RA

1. Open the RA services page.

   ```
   https://server.example.com:12889/services
   ```

2. Click the **Administrator Services** link.
3. Click the **New Group** link.
4. Fill in the group ID and the name of the group; the name can be longer than the GID, more like a description, to help differentiate the group.



5. Click the **`Add New Group`** link at the top of the form.
6. After the group is created, add it to the RA configuration so that the group has agent or administrative functions.
    a. Stop the RA instance.

    ```
    service pki-ra stop
    ```

    Always stop a subsystem before editing the subsystem configuration files.
    b. Open the **`CS.cfg`** file.

    ```
    vim /var/lib/pki-ra/conf/CS.conf
    ```

    c. Add the new group's GID to the adminsitrator or agent group list.

    ```
    admin.authorized_groups=administrators,example
    agent.authorized_groups=administrators,agents,example
    ```

    d. Start the RA instance.

    ```
    service pki-ra start
    ```

6.5.1.3. Adding and Removing Users in an RA Group

When a group is created, it does not have any members. Likewise, as new users are added, they have to be added to a group for them to be granted any privileges to the RA.

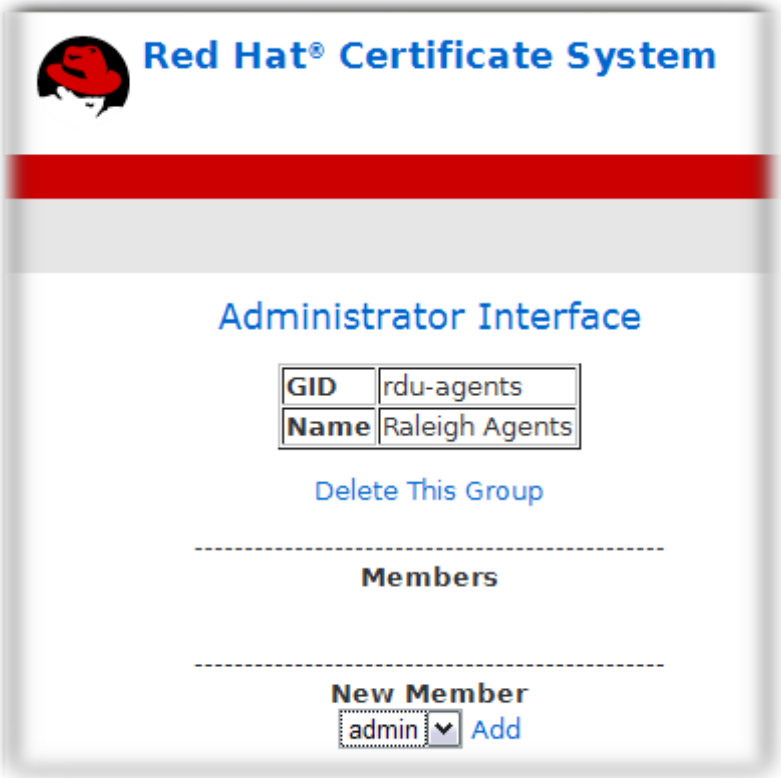
1. Open the RA services page.

    ```
    https://server.example.com:12889/services
    ```

2. Click the **`Administrator Services`** link.
3. Click the **`List Groups`** link.
4. Click the name of the group for which to change the group membership.

5. In the group page, each current member of the group is listed, with a **[Delete]** link next to the name.

   Existing members who are not members of the group are listed in a drop-down menu. To add a member, select them from the name from the menu, and click **Add**.



6.5.2. Managing RA Users

RAs have two distinct types of users: agents and administrators.

There is a division between agent tasks and administrative tasks, even though both sets of functions are accessed through web serivces pages. RA agent tasks manage operations related to issuing certificates, like approving requests. RA administrator tasks relate to managing the server instance,

mainly managing users and groups.

For an RA user to be able to perform their tasks, the user entry must be created and then added to the appropriate group.

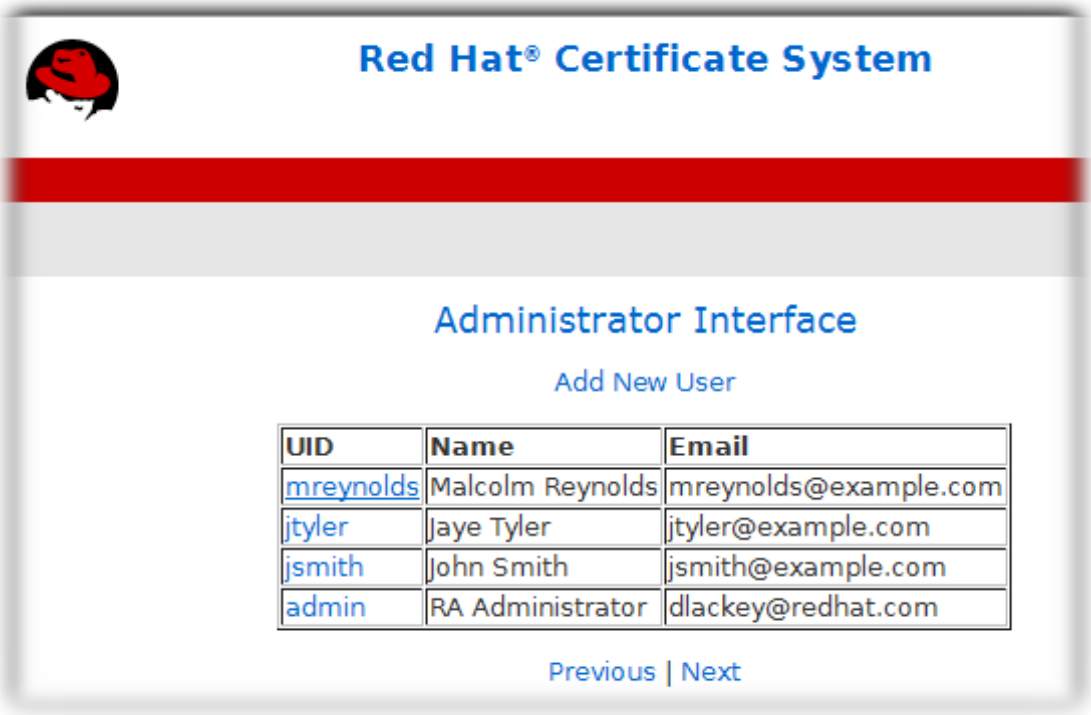
A default user is created when the RA is first configured, and this admin user belongs to both the agent and adminsitrator groups.

6.5.2.1. Listing and Viewing Users for an RA

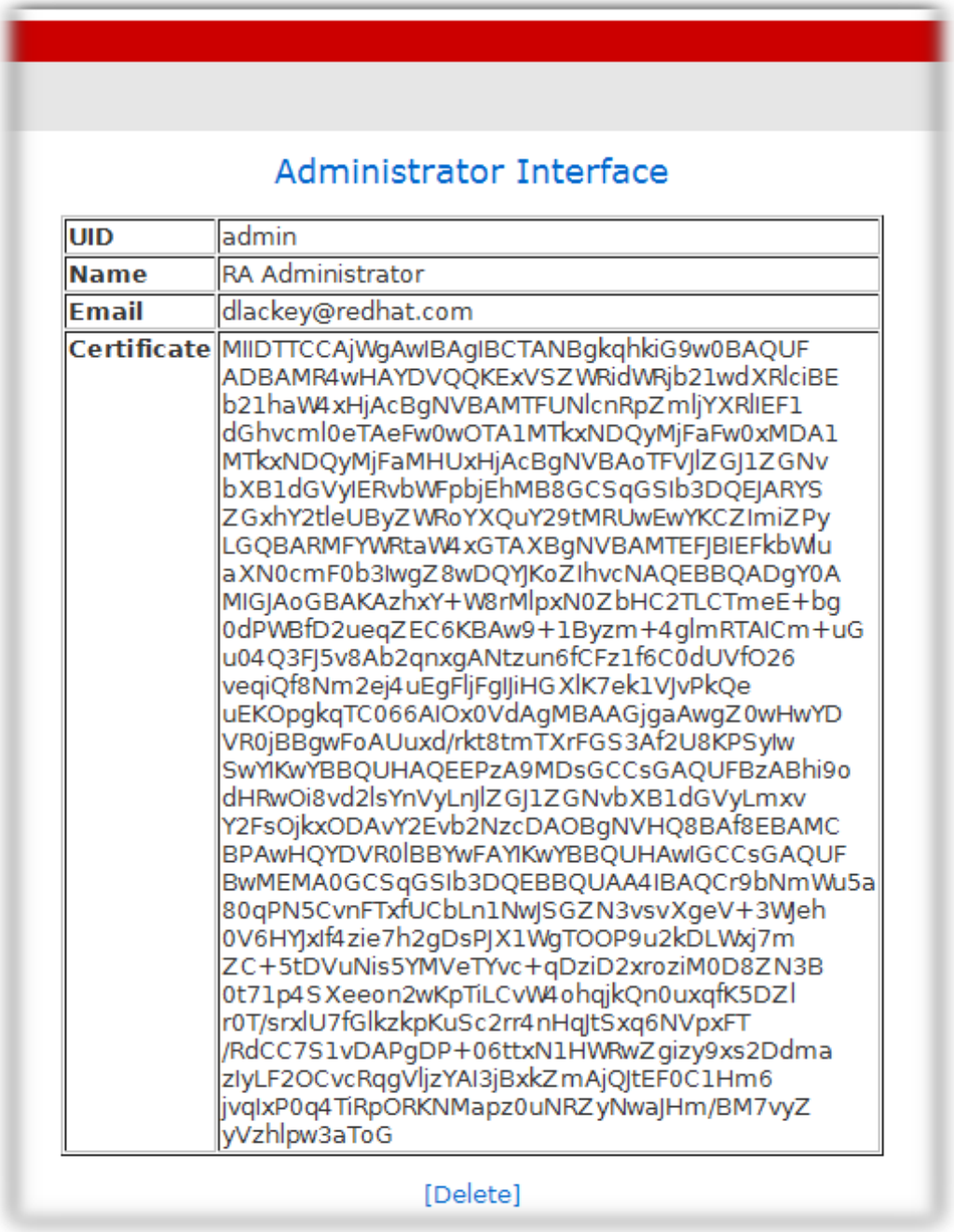
1. Open the RA services page.

```
https://server.example.com:12889/services
```

2. Click the **Administrator Services** link.
3. Click the **List Users** link.
4. All of the configured users for the RA are shown. To view a user, click the UID for that user.



5. The user details page shows the person's UID, full name, email address, and user SSL certificate.



6.5.2.2. Creating a New User for an RA

1. Generate a new certificate for the user. All access to the RA web services pages is done through certificate-based authentication, so all RA agents and administrators must have a certificate. This is covered in Section 6.5.2.3, “Generating Agent Certificates for RA Agents”.
2. Open the RA services page.

   ```
   https://server.example.com:12889/services
   ```

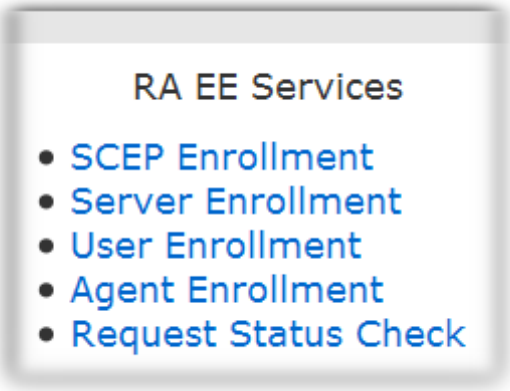
3. Click the **Administrator Services** link.
4. Click the **New User** link.
5. Fill in the user ID, full name, and email address of the user, and paste in the base 64-encoded certificate requested in the first step.

6. Click the **`Add New User`** link at the bottom of the form.
7. Once the user is created, add him as a member to the appropriate group so that the user can perform any RA agent or administrator functions. Adding members to groups is covered in Section 6.5.1.3, “Adding and Removing Users in an RA Group”.

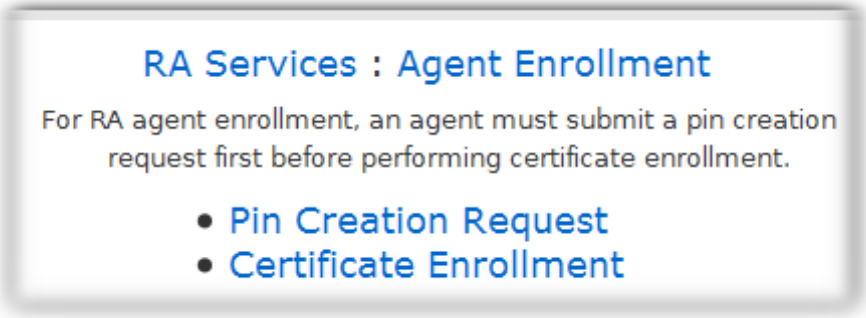
6.5.2.3. Generating Agent Certificates for RA Agents

RA agents must have a client certificate that allows them to authenticate to the RA subsystem (meaning accessing the RA agent and administrator services pages). Any SSL client certificate can be used, as long as it is added to the RA's SQLite database, but it is easier to use the default enrollment process in the RA services page.

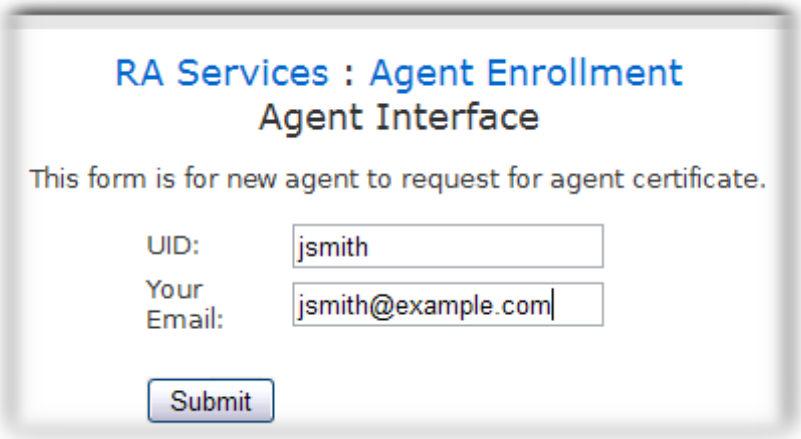
1. Request a one-time PIN to use as a certificate request.
    a. Click **`SSL End Users Services`** to open the request submission page.
    b. Click **`Agent Enrollment`**.



    c. Click **`PIN Creation Request`**.

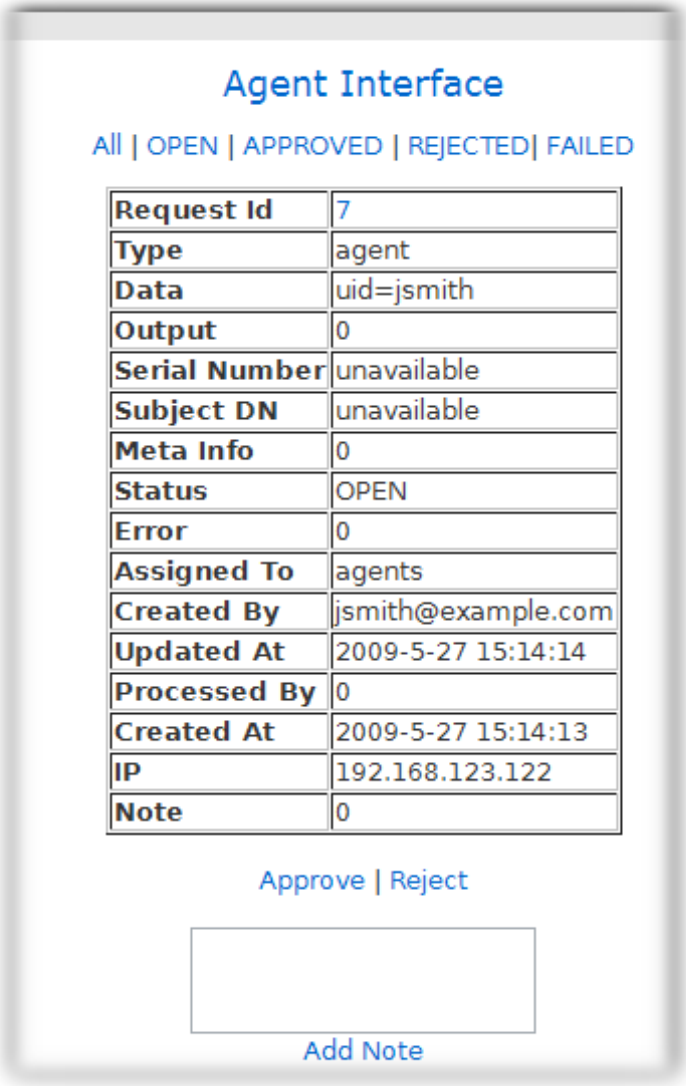

RA Services : Agent Enrollment
For RA agent enrollment, an agent must submit a pin creation request first before performing certificate enrollment.
Pin Creation Request
Certificate Enrollment

d. Enter an appropriate UID and email address.

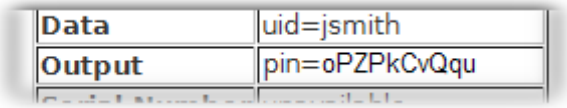


By default, notifications are enabled for the RA subsystem, so as soon as the certificate request is submitted, a notification is sent to the agent queue.

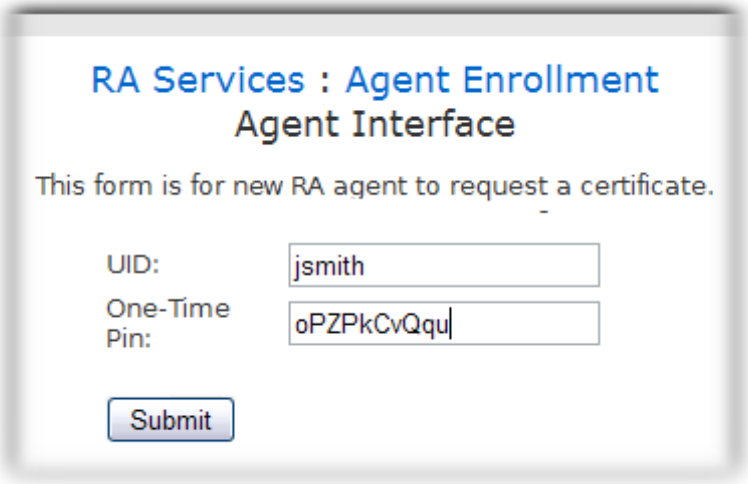
2. An existing agent must approve the PIN request.
   a. Open the agent services page.
   b. Click **`List Requests`**. The PIN request is listed in a table with a status of OPEN.
   c. Click the **`Request ID`** to display the details of the request.



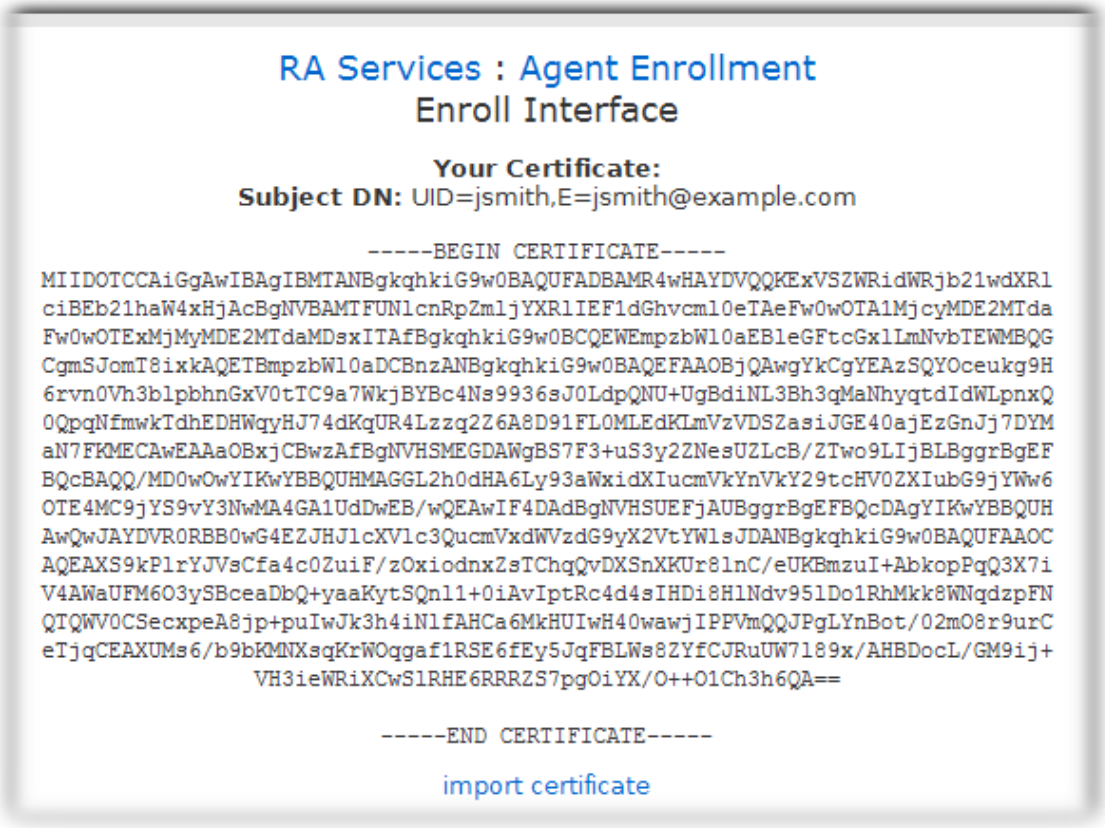
d. Click **Approve** to approve the request. This generates the PIN the user will use to retrieve the certificate.



3. The last step is for the user to use the generated PIN to retrieve his certificate.
   a. Open the **SSL End Users Services** page.
   b. Click **Request Status Check**.
   c. In the **Request ID** field, enter the ID of the PIN request.
   d. Click the value in the **Import Certificate** field to display the one-time PIN.
   e. Click **Agent Enrollment** again, and then click the **Certificate Enrollment** link.
   f. Enter the user ID and the PIN.



g. When the certificate is successfully generated, base-64 encoded blob is displayed.



Chapter 7. DRM: Recovering Encrypted Data

This chapter describes how authorized Data Recovery Manager (DRM) agents process key recovery requests and recover stored encrypted data when the encryption key has been lost. This service is available only when the DRM subsystem is installed.

7.1. Listing Requests

There are three kinds of key service requests:

- Key archival requests, made by Certificate Manager agents
- Key recovery requests, made by DRM agents
- Token key requests for archiving smart card (token) keys in conjunction with server-side key generation requests. This request can only be initiated through a TPS subsystem.

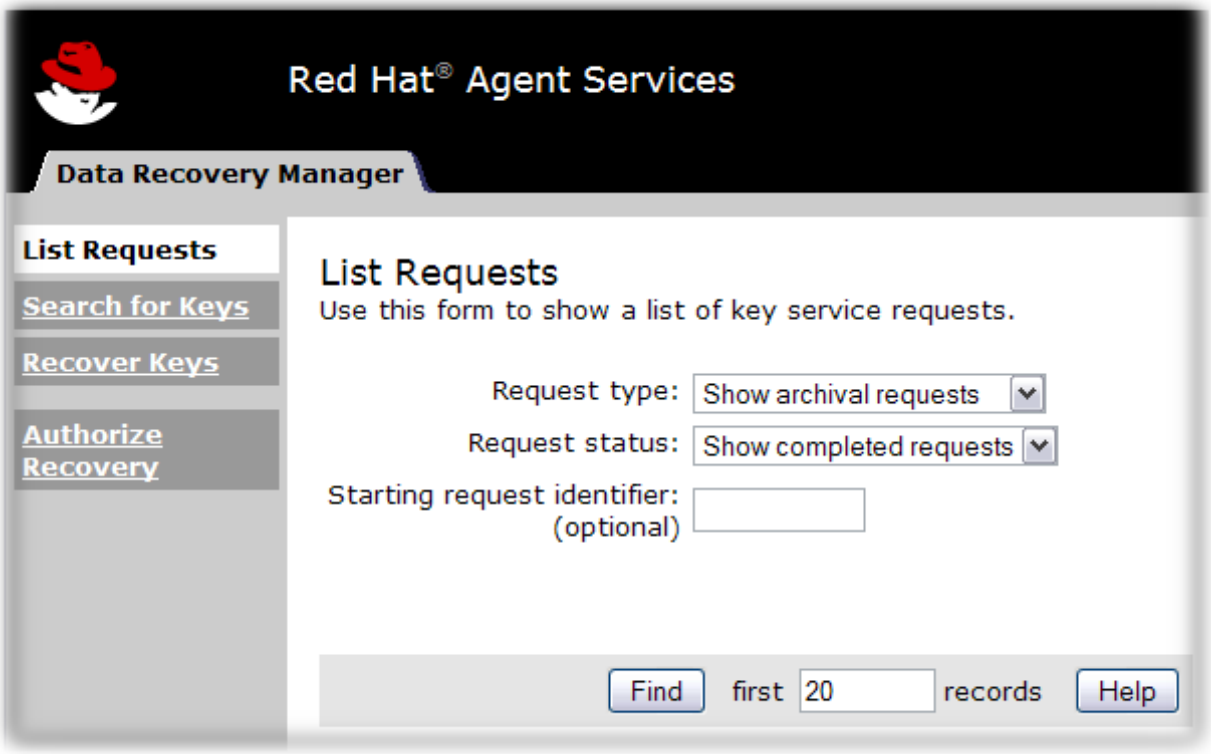
A DRM agent reviews these requests. An agent can search for and list key service requests with a particular status, such as completed or rejected, select a key service request from the returned list, and examine the request details. Key service requests are handled internally; it is not necessary to take any action on them unless the Certificate System is specially configured.

To list key service requests:

1. Open the DRM agent services page.

   ```
   https://server.example.com:10443/kra/agent/kra
   ```

2. Click **`List Requests`** to display the **`List Requests`** form.
3. Choose the type of requests to see from the **`Request type`** menu.



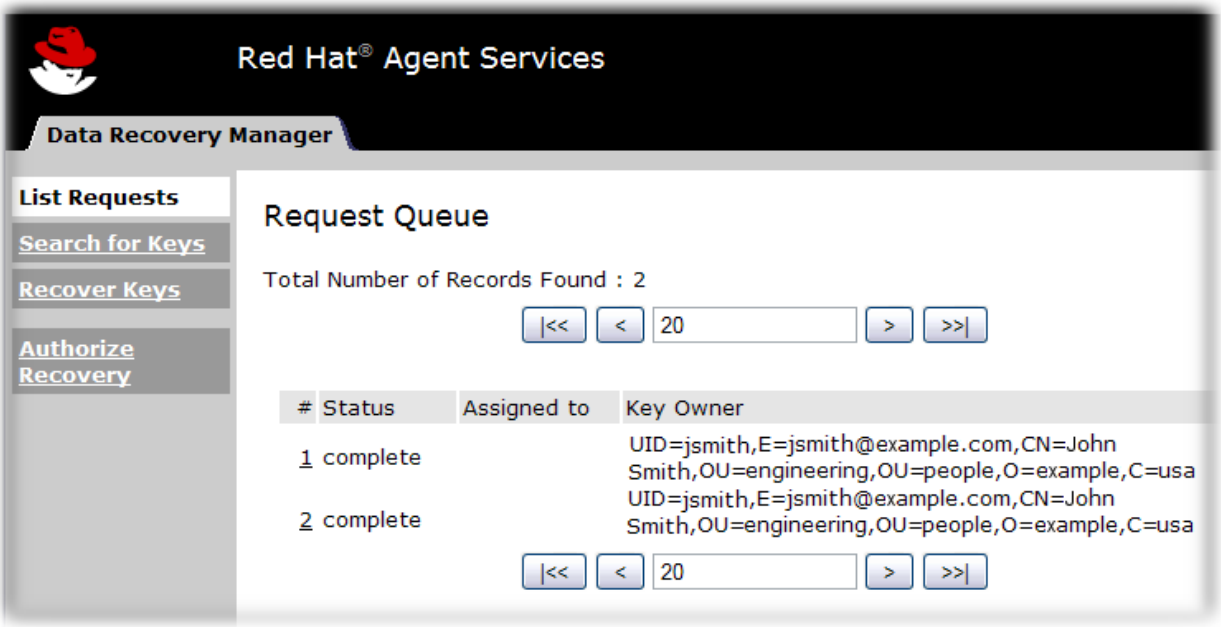
There are three request types:

- Show Key Archivals requests
- Show Key Recovery requests

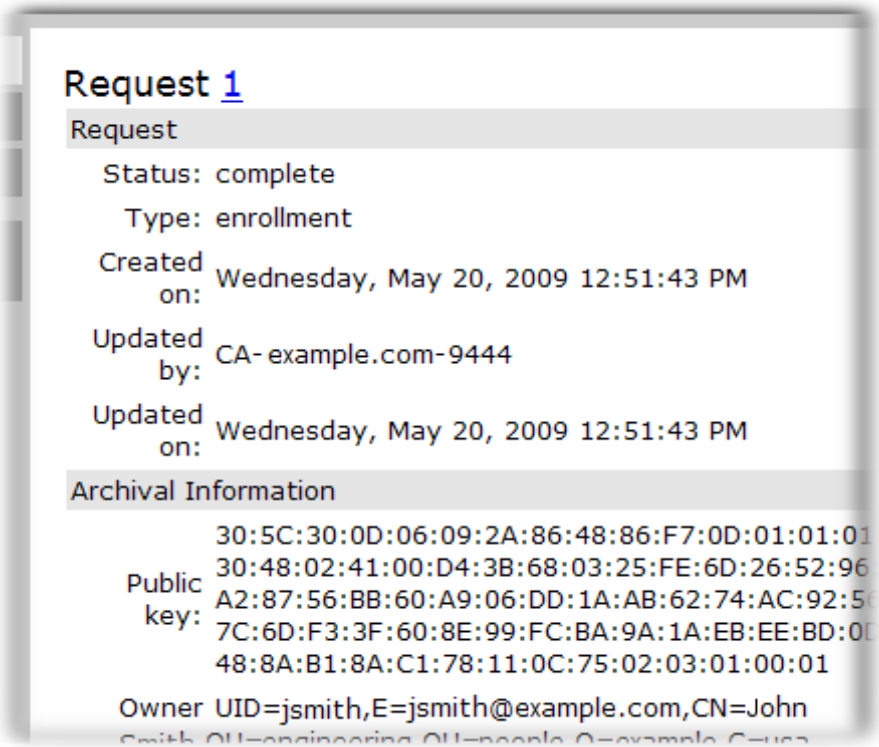
- Show Token Key requests
- Show all requests

4. Select the status of requests from the **Request status** menu.
   - *Show canceled requests.* Unless the system is specially configured to allow requests to be canceled, there are no canceled requests.
   - *Show rejected requests.* Rejected requests do not comply with the archival or recovery policies. Unless the system is specially configured to allow requests to be rejected, there are no rejected requests.
   - *Show completed requests.* Completed requests include archival requests for which proof of archival has been sent and completed recovery requests.
   - *Show all requests.* All requests stored in the system.
5. To start the list at a specific place in the queue, enter the starting request identifier in decimal form.

   Key identifiers are displayed in hexadecimal form in the **Search Results** and **Details** pages.
6. Click **Find**.
7. The DRM displays a list of the key service requests that match the search criteria. Select a request from the list to examine it in more detail.



8. On the **Key Service Request Queue** form, find a particular request. If the desired request is not shown, scroll to the bottom of the list, and use the arrows to move to another page of search results.
9. Clicking the ID number next to a request opens the **Request Details** page, which gives the complete information for the request. The request cannot be modified in this page.



NOTE

If the system changes the state of the displayed request, using the browser's **Back** or **Forward** buttons or the history to navigate through the pages can cause the data shown to become out of date. To refresh the data, click the highlighted key identifier at the top of the page.

7.2. Finding Archived Keys

Archived keys can be searched to examine the key details or to initiate recovery. Selecting search criteria and selecting a key from the search results is the same for both operations.

To search for and list archived keys:

1. Open the DRM agent services page.
2. Click **Search for Keys** or **Recover Keys** to display the search criteria form.

   When selecting the **Recover Keys** operation, there is an additional option to initiate recovery for any key that is found.

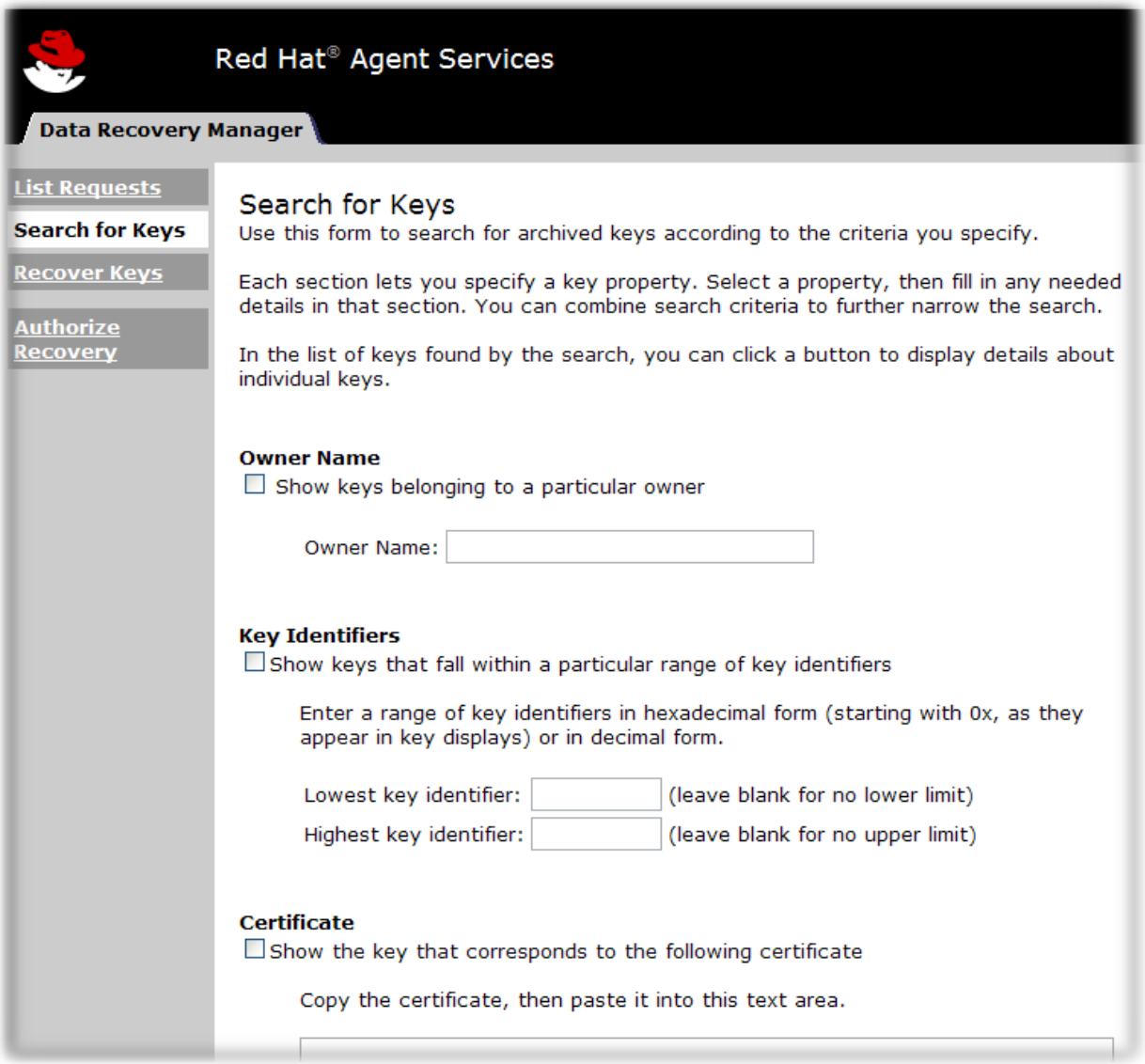

Red Hat® Agent Services
Data Recovery Manager
List Requests
Search for Keys
Recover Keys
Authorize Recovery
Search for Keys
Use this form to search for archived keys according to the criteria you specify.
Each section lets you specify a key property. Select a property, then fill in any needed details in that section. You can combine search criteria to further narrow the search.
In the list of keys found by the search, you can click a button to display details about individual keys.
Owner Name
Show keys belonging to a particular owner
Owner Name:
Key Identifiers
Show keys that fall within a particular range of key identifiers
Enter a range of key identifiers in hexadecimal form (starting with 0x, as they appear in key displays) or in decimal form.
Lowest key identifier: (leave blank for no lower limit)
Highest key identifier: (leave blank for no upper limit)
Certificate
Show the key that corresponds to the following certificate
Copy the certificate, then paste it into this text area.

Figure 7.1. Search for Keys Page

3. To search by particular criteria, use the different sections of the **`Search for Keys`** or **`Recover Keys`** form. To use a section, select the check box for that section, then fill in any necessary information.
   - *Owner name.* Finds an archived key with a specific owner name. The owner name for a key, like the subject name for a certificate, consists of a string that can be used in searches.

     NOTE

     Certificate System certificate request forms support all UTF-8 characters for the common name (owner name), and the common name field is included in the subject name of the certificate. This means that the searches for subject names or the common name in the subject name support UTF-8 characters.

   - *Key identifiers.* Finds an archived key with a specific key identifier or to list all keys within a range of key identifiers.
     - To find a key with a specific key identifier, enter the key identifier in both the upper limit and

lower limit fields in decimal or hexadecimal form. Use **0x** to indicate the beginning of a hexadecimal number; for example, **0x2A**. Key identifiers are displayed in hexadecimal form in the **Search Results** and **Details** pages.

- To find all keys within a range of key identifiers, enter the upper and lower limits of the key identifier range in decimal or hexadecimal form.

Leaving either the lower limit or upper limit field blank displays all keys before or after the number specified.

- *Certificate.* Finds the archived key that corresponds to a specific public key. Select the check box and paste the certificate containing the base-64 encoded public key into the text area.

NOTE

The encryption certificate associated with the key pair must be found first. Use the Certificate Manager agent services page to find the certificate; for instructions, see Section 4.3, “Examining Certificate Details”.

- *Archiver.* Finds keys that were archived by a specific server. Select the check box and enter the user ID of the Certificate Manager that submitted the key archival request. This information is available only for archival requests from servers that are remote from the DRM. To put a limit on the number of results returned, fill in a value for maximum results. To limit the time allowed for the search, enter a value for time limit in seconds.

4. After entering the search criteria, click **Show Key**.

The DRM displays a list of the keys that match the search criteria. Select a key from the list to examine its details. If the search was initiated with the **Recover Keys** button, there is the additional option of recovering any key returned by the search.

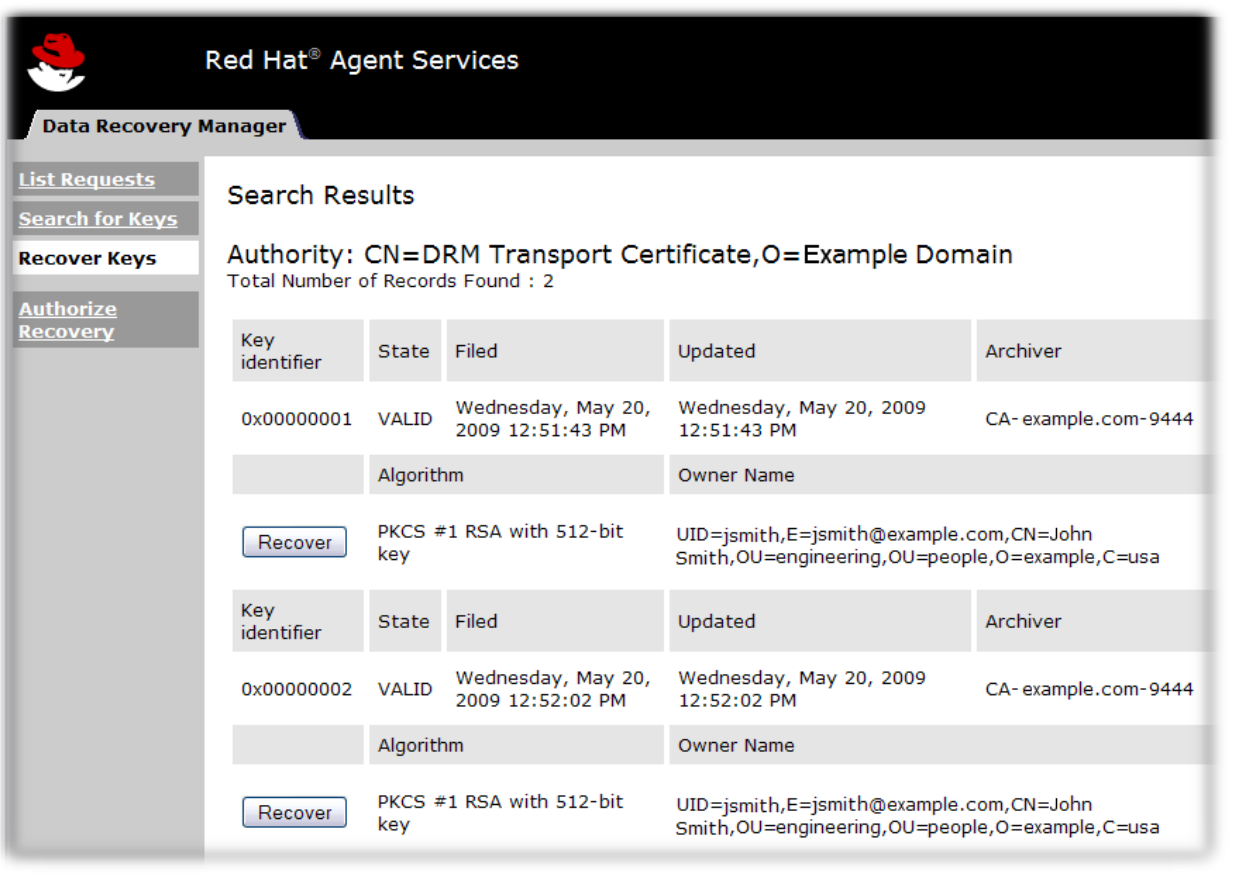


Figure 7.2. Search Results Page

5. In the **`Search Results`** form, select a key.

   If a desired key is not shown, scroll to the bottom of the list and use the arrows to move to another page of search results.
6. Click the ID number next to the selected key. The details of the selected key are shown in the **Key** details page. It is not possible to modify the key through this page.

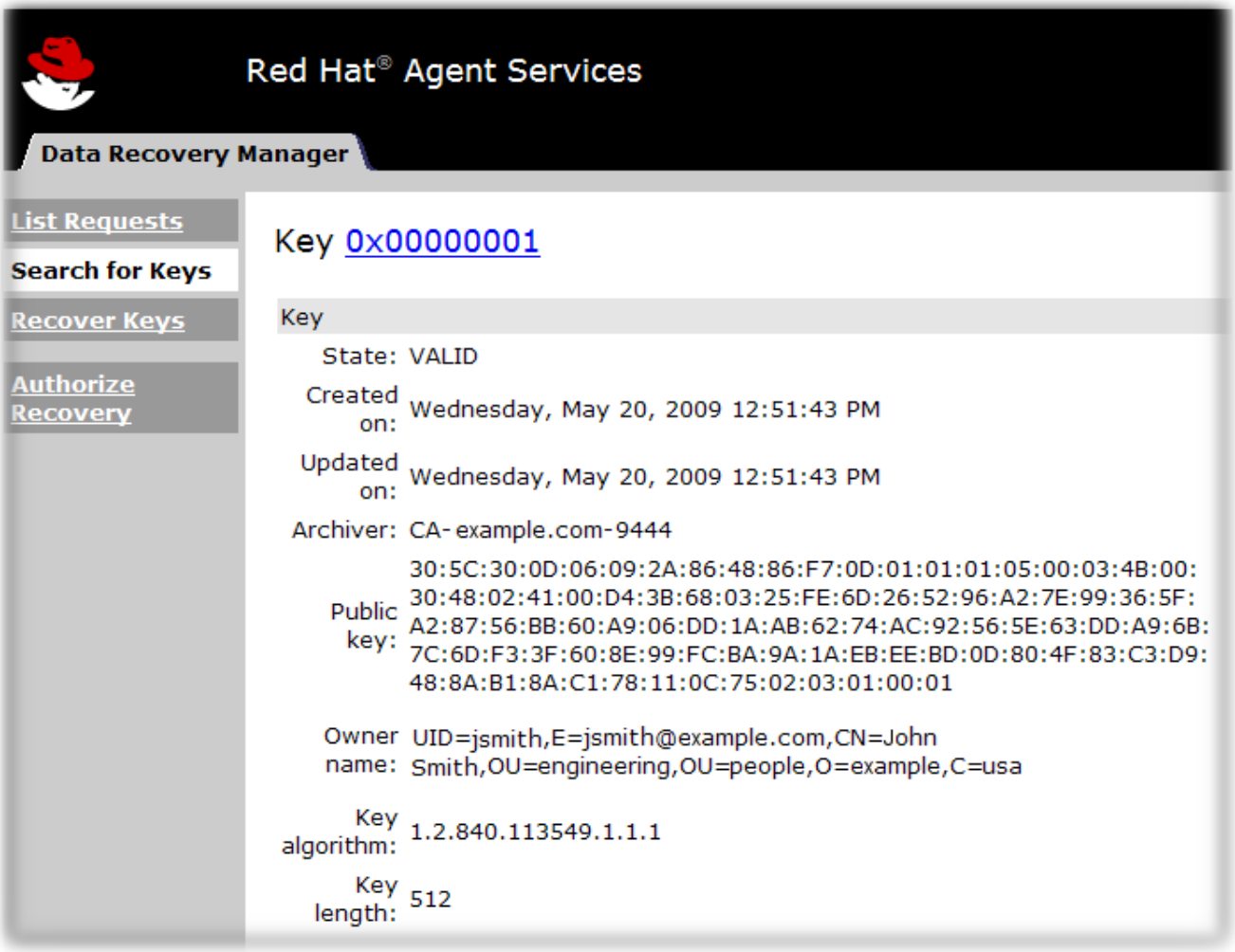


Figure 7.3. Key Details Page

7.3. Recovering Keys

If an end user loses a private encryption key or if a key's owner is unavailable, data encrypted with that key cannot be read unless a copy of the private key was archived when the key was created. The archived key can then be recovered and used to read the data.

A DRM agent manages key recovery through the DRM agent services page. Archived keys can be searched to view the details or to initiate a key recovery. Once a key recovery is initiated, a minimum number of designated DRM agents are required to authorize the recovery.

There are two different paths for key recovery.

- *Synchronous recovery* means that when the first agent initiates the key recovery process, the process persists and the original browser must remain open until the entire process is complete. When the agent starts the recovery process, the DRM returns a reference number. All subsequent agents use the **`Authorize Recovery`** area and that referral link to access the thread. Continuous updates on the approval status are sent to the initiating agent so they can check the status.

IMPORTANT

If the original session is lost, such as the browser is closed or the DRM shuts down, then the entire recovery process must be restarted.

- *Asynchronous recovery* means that each step of the recovery process — the initial request and each subsequent approval or rejection — is stored in the DRM's internal database, under the key entry. The data for the recovery process can be retrieved even if the original browser session is closed or the DRM is shut down. Agents search for the key to recover, without using a reference number.

These two recovery options are illustrated in Figure 7.4, “Async and Sync Recovery, Side by Side”.

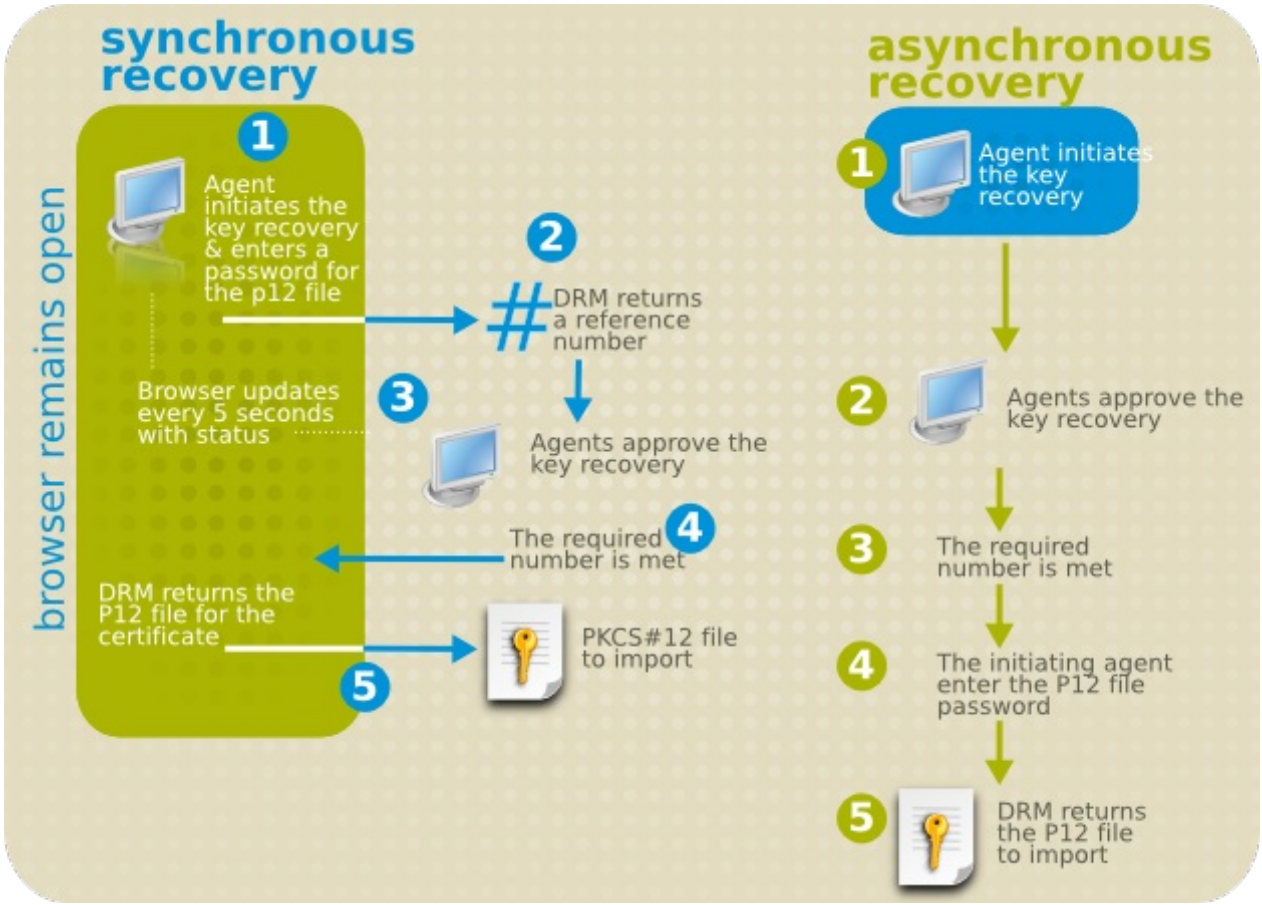


Figure 7.4. Async and Sync Recovery, Side by Side

NOTE

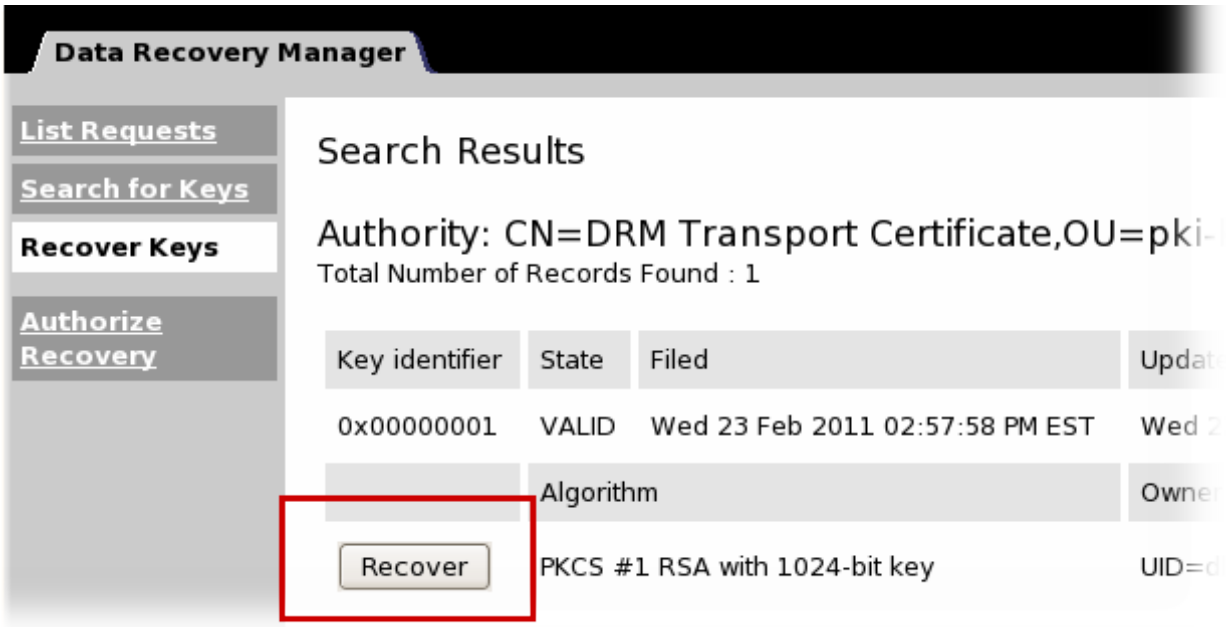
This section describes how to recover keys that are not stored on a smart card. For smart card key recovery, see Chapter 9, *TPS: Managing Token and Smart Card Operations*.

7.3.1. Recovering Keys: Asynchronous Recovery

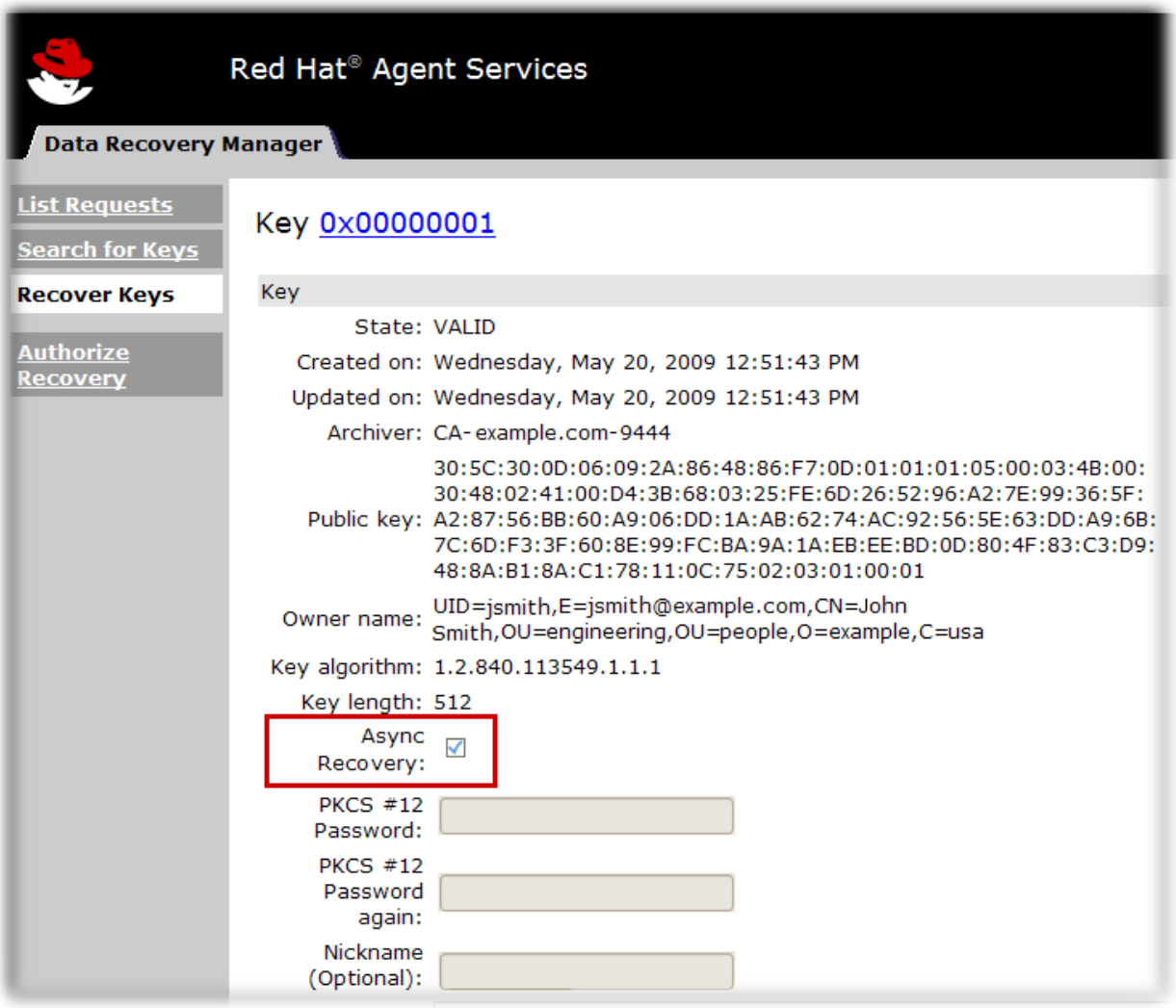
7.3.1.1. Initiating Key Recovery

1. On the DRM agent services page, click **Recover Keys**, specify search criteria, and click **Show Key** to display a list of archived keys.
2. In the **Search Results** form, select a key.

   If a desired key is not shown, scroll to the bottom of the list and select **Next** or **Previous** for another page of search results.
3. Click **Recover** next to the selected key.

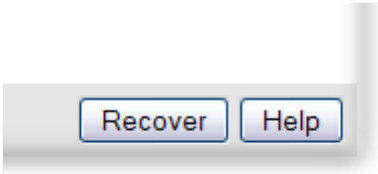


4. Check the **Async Recovery** checkbox.

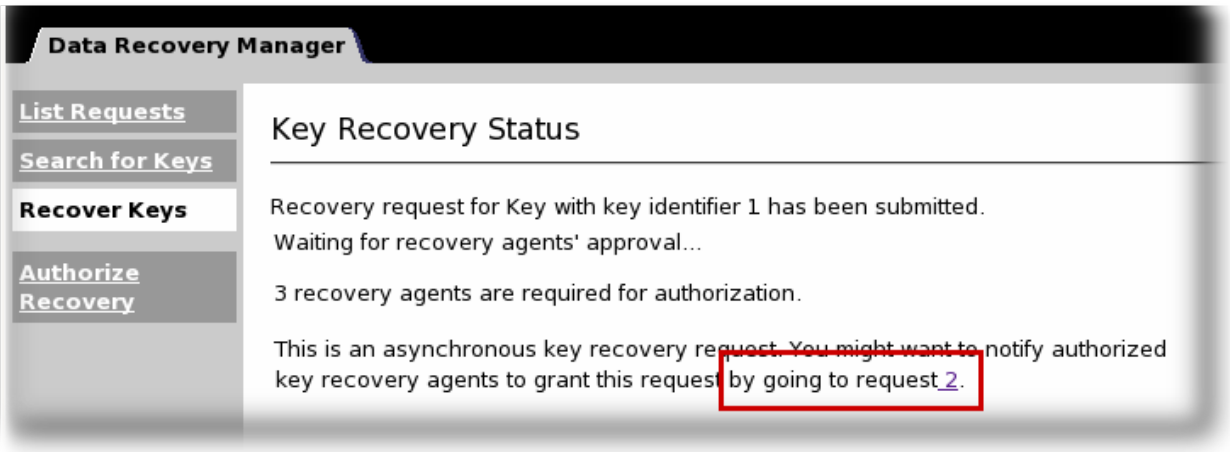


5. Paste the base-64 encoded certificate corresponding to the archived key into the text area. (The certificate can be searched and viewed through the Certificate Manager agent services pages.)

   If the archived key was found through the corresponding public key, the certificate information is automatically transferred to the form.
6. Click **Recover** to initiate the key recovery request.



7. The DRM returns a link that goes directly to the page for the key to recover. This URL can be given to other recovery agents, or they can search for the key in the **Recover Keys** page.


Data Recovery Manager
List Requests
Search for Keys
Recover Keys
Authorize Recovery
Key Recovery Status
Recovery request for Key with key identifier 1 has been submitted.
Waiting for recovery agents' approval...
3 recovery agents are required for authorization.
This is an asynchronous key recovery request. You might want to notify authorized key recovery agents to grant this request by going to request 2.

The browser can be closed as the recovery approval process goes on.

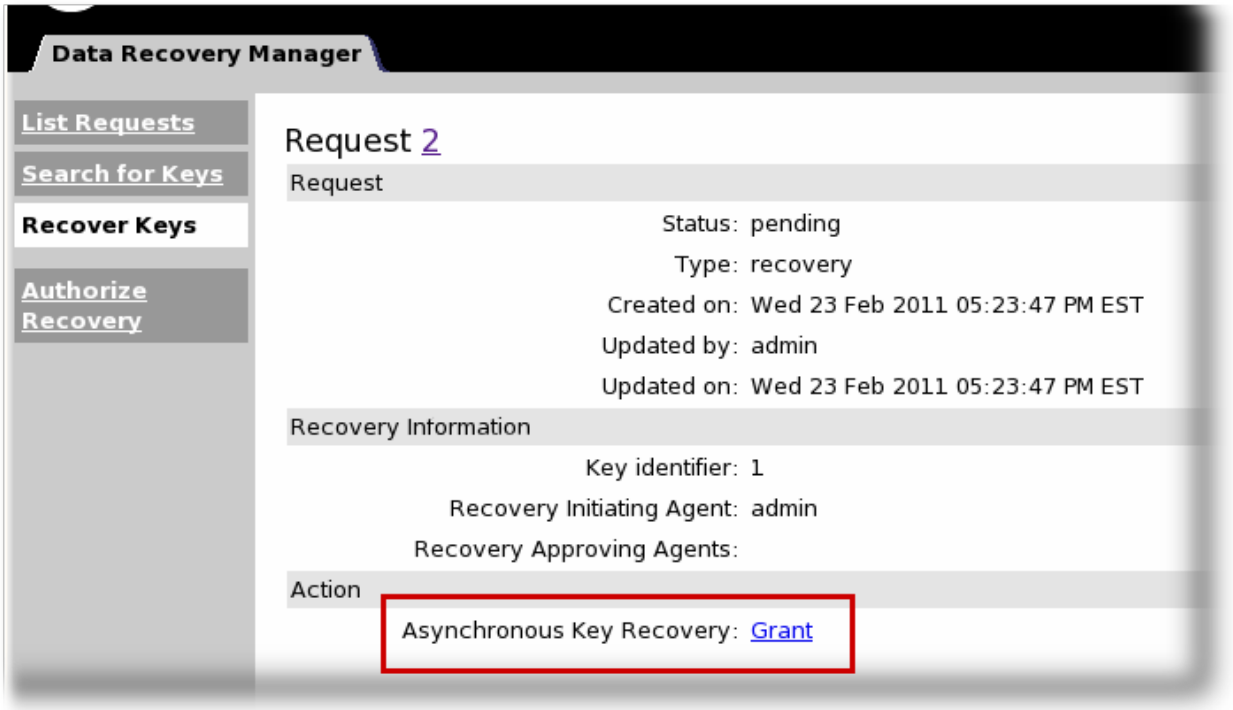
7.3.1.2. Getting Agent Approval for Key Recovery

Every DRM agent must approve the key recovery.

1. Open the DRM agent services page.

```
https://server.example.com:10443/kra/agent/kra
```

2. Either go to the URL that was returned when the request was initiated or search for the key in the **Recover Key** area.
3. The details for the recovery are shown on the key's detail page. Click the **Grant** link to approve the key recovery.



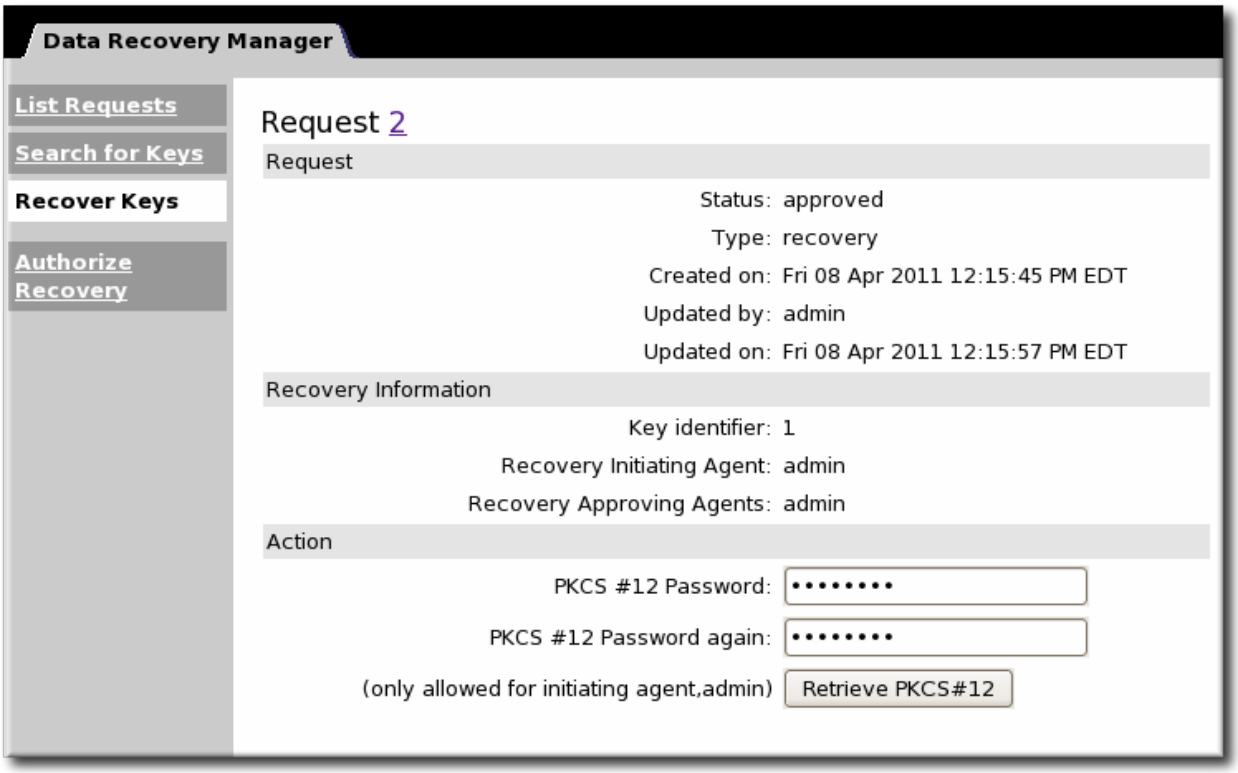
7.3.1.3. Recovering the Key

A recovery can only be performed after the required number of agents (by default, one) have approved the recovery request.

1. Search for the key recovery request, as in Section 7.1, “Listing Requests”.

> **NOTE**
>
> The recovery must be done by the initiating agent.

2. Enter and confirm a password to use to encrypt the PKCS #12 file, and click the **Retrieve PKCS #12** button.



3. Specify the path and filename to save the encrypted file containing the recovered certificate and key pair.
4. Send the encrypted file to the requester.
5. Give the recovery password to the requester in a secure manner. The requester must use this password to import the recovered certificate/key pair.

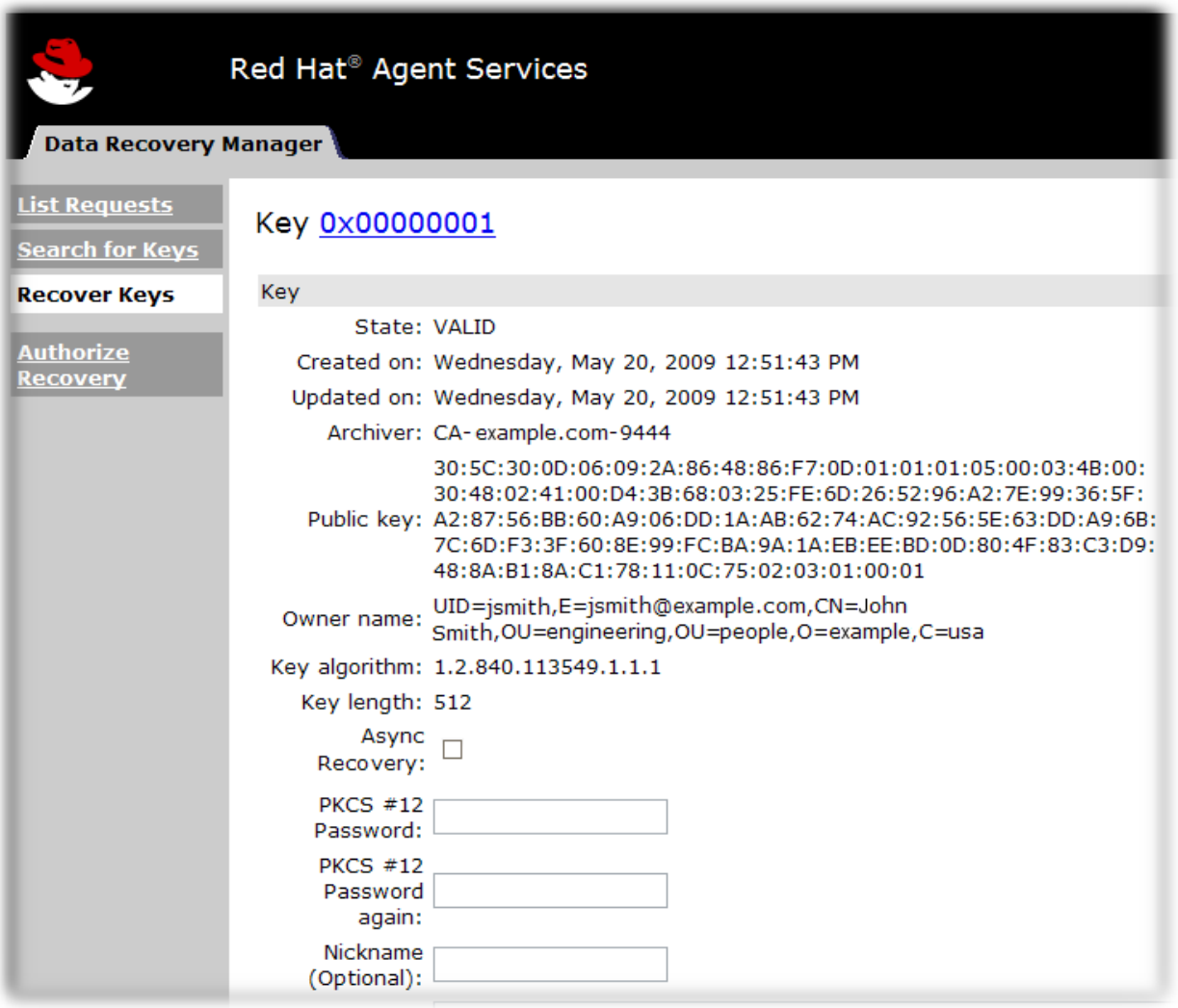
7.3.2. Recovering Keys: Synchronous Recovery

7.3.2.1. Initiating Key Recovery

1. On the DRM agent services page, click **Recover Keys**, specify search criteria, and click **Show Key** to display a list of archived keys.
2. In the **Search Results** form, select a key.

   If a desired key is not shown, scroll to the bottom of the list and select **Next** or **Previous** for another page of search results.
3. Click **Recover** next to the selected key.

   The key details are displayed in the **Authorize Key Recovery** form, where the agent submits authorization information.

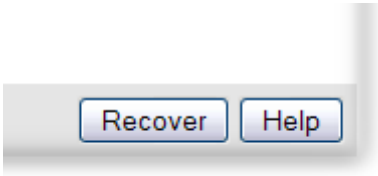


The number of key recovery agent authorizations required to recover a key is configured by the DRM administrator by setting the following parameters in the **CS.cfg** file.

```
kra.noOfRequiredRecoveryAgents=1
kra.recoveryAgentGroup=Data Recovery Manager Agents
```

4. Set the PKCS #12 token password that the requester uses to import the recovered certificate/key pair package.
5. Optionally, set a certificate nickname for the archived key.
6. Paste the base-64 encoded certificate corresponding to the archived key into the text area. (The certificate can be searched and viewed through the Certificate Manager agent services pages.)

   If the archived key was found through the corresponding public key, the certificate information is automatically transferred to the form.
7. Click **Recover** to initiate the key recovery request.



Selecting this option notifies the key recovery agents that a recovery has been initiated and gives them the recovery authorization reference number. The recovery authorization reference number is listed at the top of the page.

NOTE

Do not close the browser after initiating the key recovery. The agent must wait for all other agents to authorize the key recovery request before the system returns the hyperlink to download the PKCS #12 file containing the private key. This page keeps refreshing to check if all other agents have authorized.

The status page opens and shows the progress of the recovery, to see how many agents have yet to approve the recovery. Leave the browser window open until all required agents have approved the recovery.

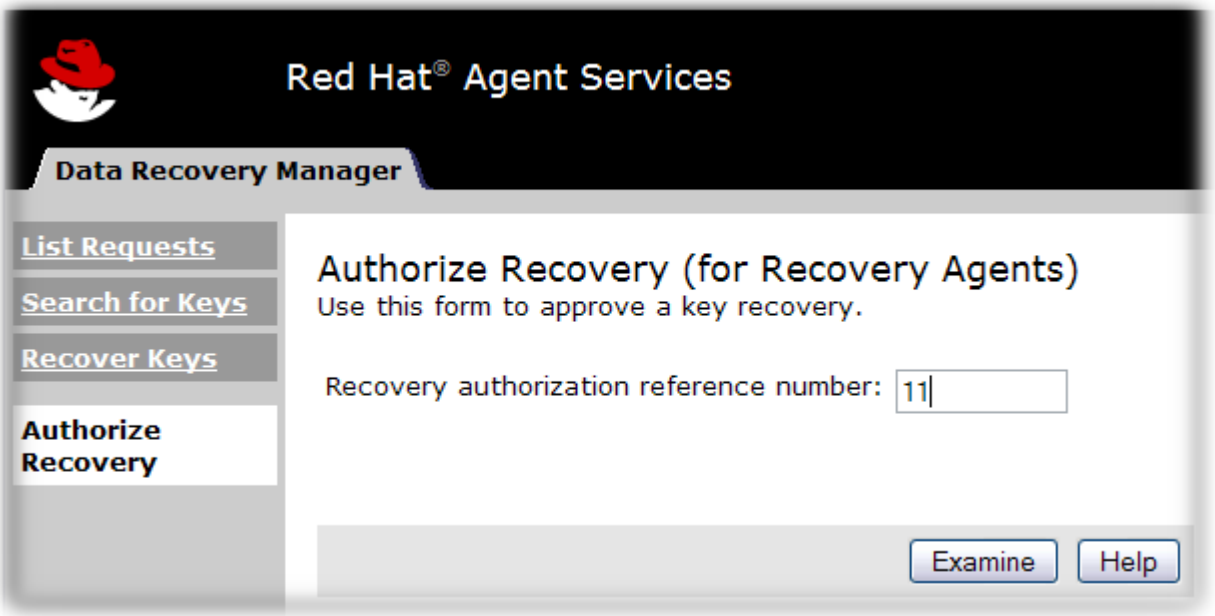
7.3.2.2. Getting Agent Approval for Key Recovery

Every DRM agent must approve the key recovery once the agent receives the recovery authorization number.

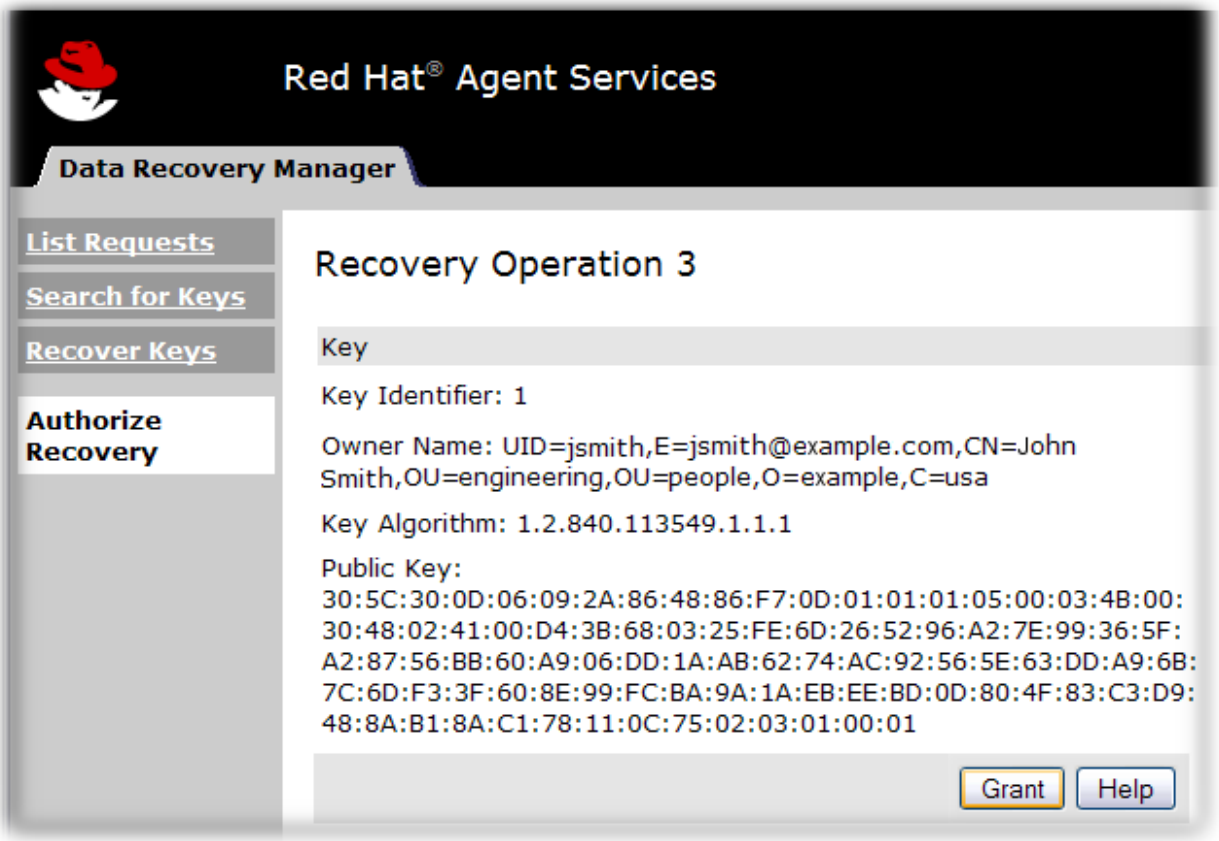
1. Open the DRM agent services page.

```
https://server.example.com:10443/kra/agent/kra
```

2. Select **`Authorize Recovery`**.
3. Enter the recovery authorization request number.



4. Select **`Examine`** to examine the key being recovered.
5. Select **`Grant`** to complete the key recovery.



7.3.2.3. Recovering the Key

1. Once all agents have authorized the recovery, then the agent who initiated the key recovery request is given a link download (import) the PKCS #12 file.
2. When selecting the PKCS #12 file, a dialog box appears. Specify the path and filename to save the encrypted file containing the recovered certificate and key pair.
3. Send the encrypted file to the requester.

4. Give the recovery password to the requester in a secure manner.
   The requester must use this password to import the recovered certificate/key pair.

Chapter 8. Online Certificate Status Manager: Verifying Certificate Status

This chapter describes how to perform Online Certificate Status Manager (OCSP) agent tasks, such as identifying a CA to the Online Certificate Status Manager and adding a CRL to the Online Certificate Status Manager's internal database. This service is available only when the Online Certificate Status Manager subsystem is installed. The Online Certificate Status Manager agent services page allows authorized agents to accomplish these tasks.

8.1. Listing CAs Identified by the Online Certificate Status Manager

The Online Certificate Status Manager can be configured to receive CRLs from multiple Certificate Managers. Each Certificate Manager that can publish CRLs to the Online Certificate Status Manager must have its CA signing certificate stored in the internal database of the Online Certificate Status Manager. For instructions, see Section 8.2, “Identifying a CA to the Online Certificate Status Manager”.

The list of Certificate Managers currently recognized by the Online Certificate Status Manager can be viewed at any time. To see the list of Certificate Managers:

1. Open the Online Certificate Status Manager agent services page.
2. In the left frame, click **`List Certificate Authorities`**.

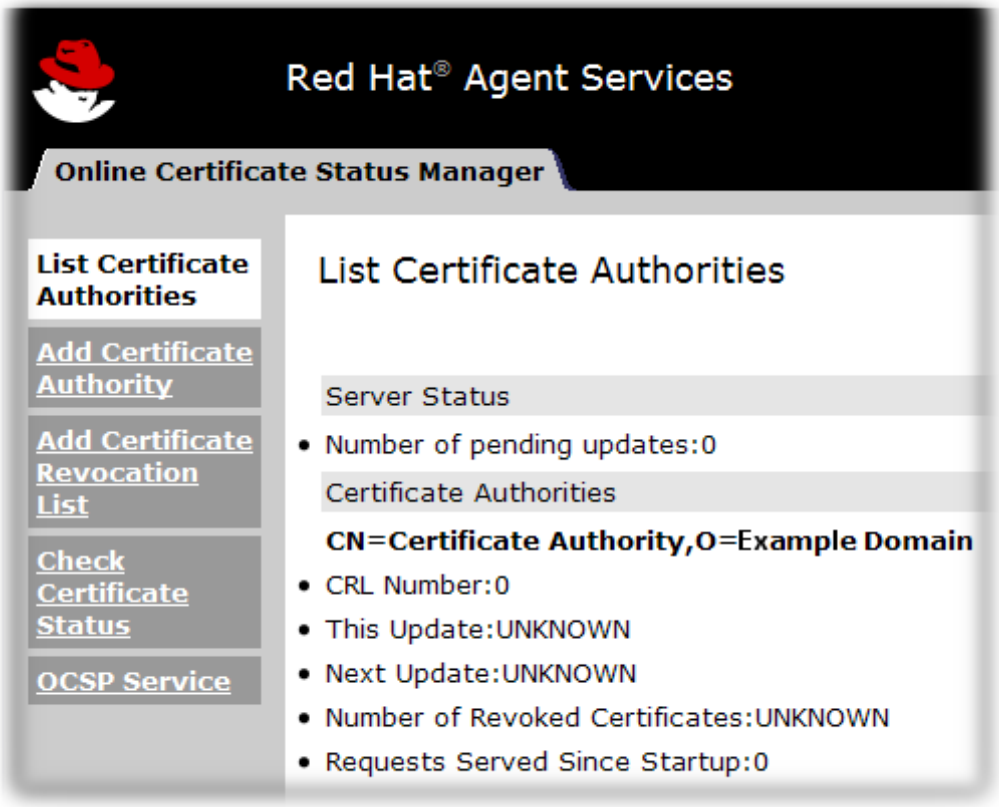


Figure 8.1. OCSP List Certificate Authorities Page

8.2. Identifying a CA to the Online Certificate Status Manager

The Online Certificate Status Manager can be configured to receive CRLs from multiple Certificate Managers. Before configuring a Certificate Manager to publish CRLs to the OCSP, first identify the Certificate Manager to the Online Certificate Status Manager by storing the Certificate Manager's CA signing certificate in the internal database of the Online Certificate Status Manager.

To store the Certificate Manager's CA signing certificate in the internal database of the Online Certificate Status Manager:

1. Open the Certificate Manager's end-entities page.

   ```
   https://server.example.com:9444/ca/ee/ca
   ```

2. Select the **Retrieval** tab, and, in the left frame, click **List Certificates**.
3. When the page opens, click **Find**.
4. Locate the Certificate Manager's CA signing certificate by looking at the subject name of the certificate. Typically, the CA signing certificate is the first certificate the Certificate Manager issues.
5. Click on the subject name.
6. In the certificate contents page, scroll to the **Base 64 encoded certificate** section, which shows the CA signing certificate in its base 64-encoded format.
7. Copy the base 64-encoded certificate, including the **-----BEGIN CERTIFICATE-----** and **-----END CERTIFICATE-----** marker lines, to the clipboard or a text file. The certificate information looks similar to this example:

   ```
   -----BEGIN CERTIFICATE-----
   MIIB/DCCAaagAwIBAgIBATANBgkqhkiG9w0BAQUFADBRMRwwGgYDVQQKExNTZmJh
   eSBSZWRoYXQgRG9tYWluMREwDwYDVQQLEwgxMDI3cm9vdDEeMBwGA1UEAxMVQ2Vy
   dGlmaWNhdGUgQXV0aG9yaXR5MB4XDTA2MTAyNzE2MTkyM1oXDTA4MTAxNjE2MTky
   M1owUTEcMBoGA1UEChMTU2ZiYXkgUmVkaGF0IERvbWFpbjERMA8GA1UECxMIMTAy
   N3Jvb3QxHjAcBgNVBAMTFUNlcnRpZmljYXRlIEF1dGhvcml0eTBcMA0GCSqGSIb3
   DQEBAQUAA0sAMEgCQQDXA7qzGv1LJNxEvlHkDKvLjr+OgHmhj4BaPAXTVw64szgT
   McQh1aY0G4plpTdCwECEiMb3JRa8QzpfRwbB/kFpAgMBAAGjaTBnMA8GA1UdEwEB
   /wQFMAMBAf8wDgYDVR0PAQH/BAQDAgHGMEQGCCsGAQUFBwEBBDgwNjA0BggrBgEF
   BQcwAYYoaHR0cDovL3Bhdy5zZmJheS5yZWRoYXQuY29tOjkwODAvY2Evb2NzcDAN
   BgkqhkiG9w0BAQUFAANBAIOhIcmHQ4HHSPQielUVx0EoiseeXL/t8VrAnK0i2uMn
   7eZlvLIXrcQAcQTI4yxavKtOtkqrPR6uV5LhCqaX2hg=
   -----END CERTIFICATE-----
   ```

8. Open the Online Certificate Status Manager agent services page.

   ```
   https://server.example.com:11443/ocsp/agent/ocsp
   ```

9. In the left frame, click **Add Certificate Authority**.
10. In the resulting form, paste the encoded CA signing certificate inside the **Base 64 encoded certificate (including header and footer)** text area.

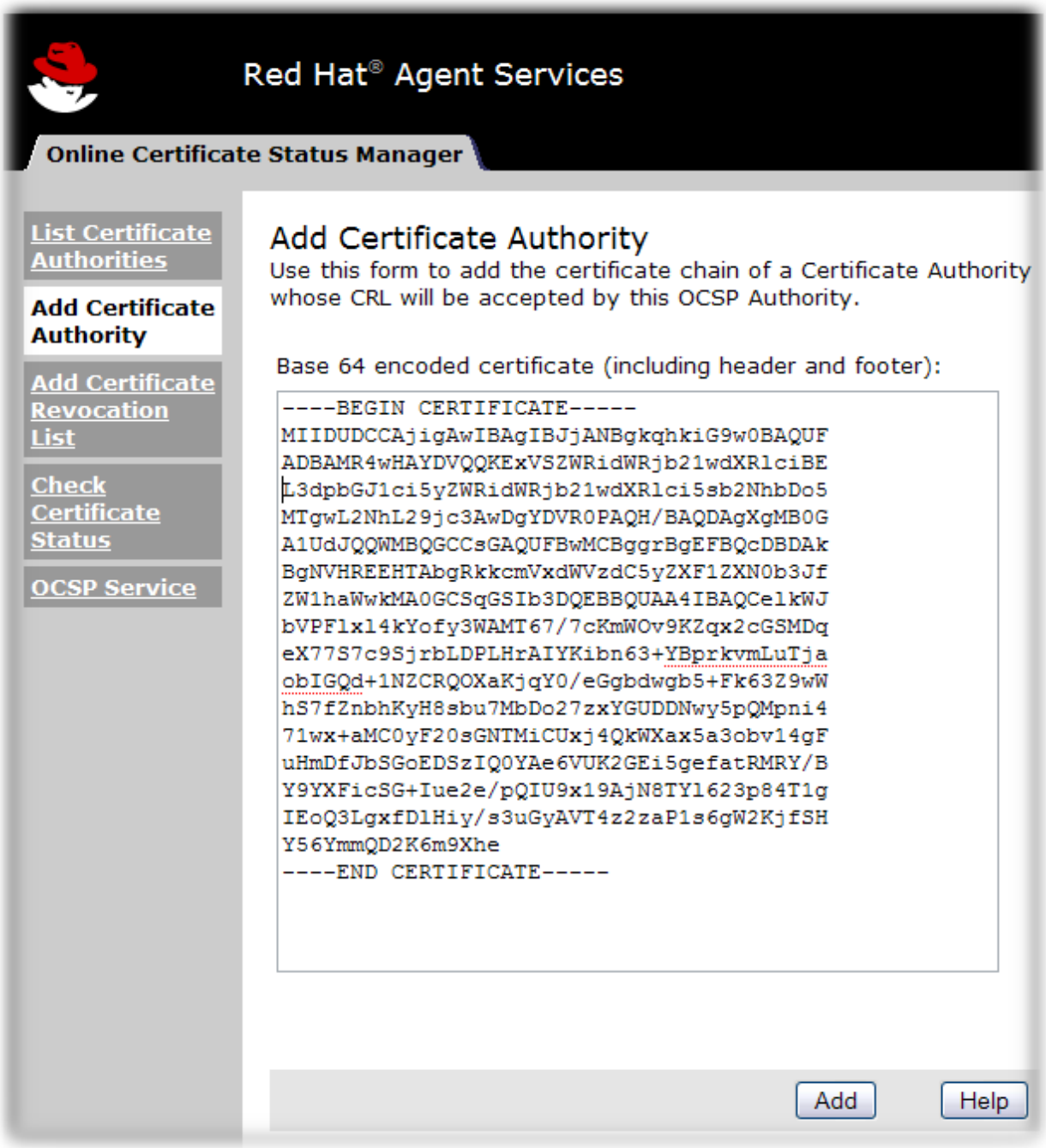


Figure 8.2. Add Certificate Authority Page

11. Click **Add**.

    The certificate is added to the internal database of the Online Certificate Status Manager.

> **NOTE**
>
> If the CA contains multiple CRL distribution points, always publish the master CRL (the CRL that contains all revoked certificates from that CA) to the OCSP responder.

12. To verify that the certificate is added successfully, click **`List Certificate Authorities`** in the left frame.

The next page shows information about the Certificate Manager that was added.

NOTE

If the deployment contains chained CAs, such as a root CA and then several subordinate CAs, add each CA certificate separately to the OCSP responder.

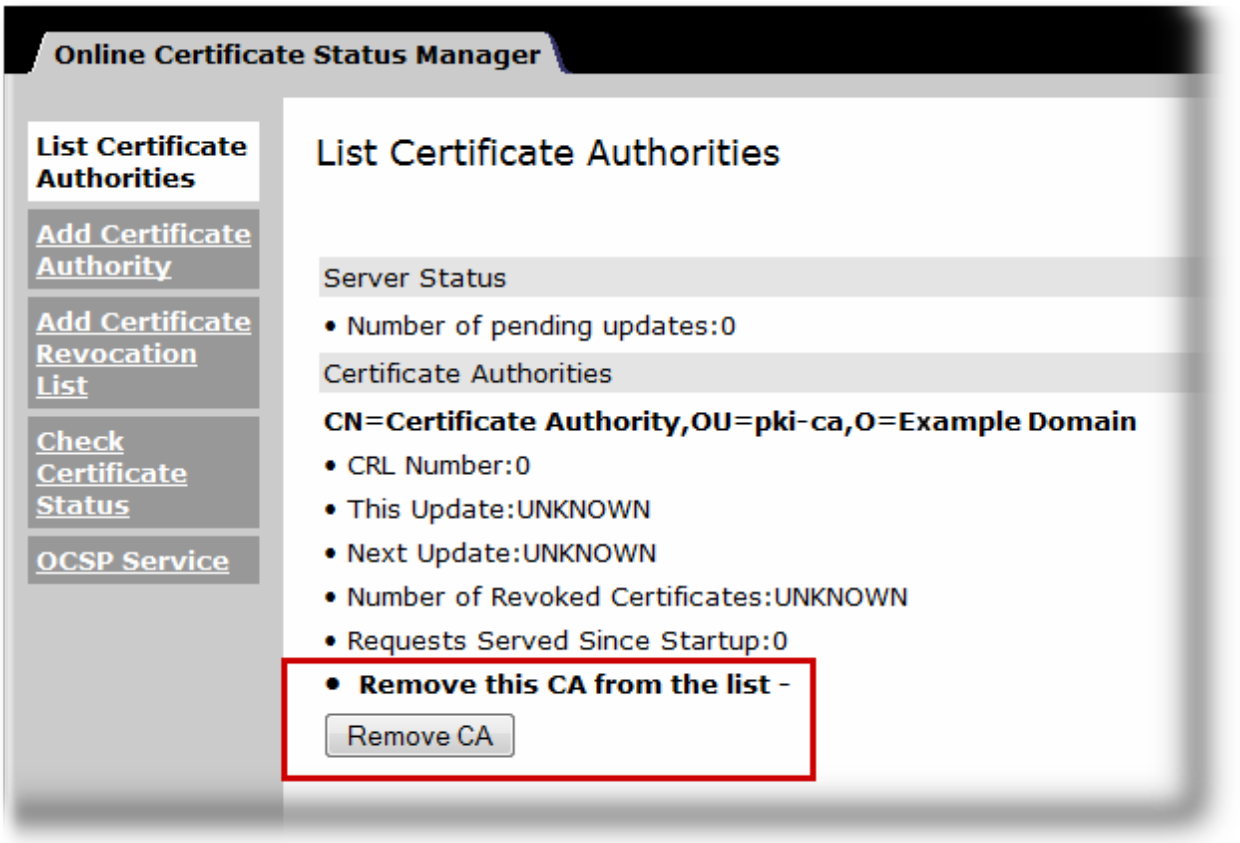
8.3. Removing a CA from the OCSP Manager

Since the CA configuration may change, CAs may need to be removed from the OCSP Manager configuration.

1. Open the Online Certificate Status Manager agent services page.

```
https://server.example.com:11443/ocsp/agent/ocsp
```

2. In the left frame, click **`List Certificate Authority`**.
3. Each of the CAs configured with the OCSP Manager has a **`Remove CA`** buttonat the bottom of the CA information. Click the button.



4. Confirm that you want to remove the CA from the OCSP Manager configuration.

8.4. Adding a CRL to the Online Certificate Status Manager

If a situation arises when a Certificate Manager is unable to publish its CRL to the Online Certificate Status Manager, it is possible to add a CRL manually to the Online Certificate Status Manager internal database.

To add a CRL to the internal database:

1. Open the Certificate Manager's agent services page.

   ```
   https://server.example.com:9444/ca/ee/ca
   ```

2. Click on **Display Revocation List**.
3. In the results page, select the desired CRL issuing point, select the option to display the CRL as base 64 encoded, and click **Display**.
4. In the CRL details page, scroll to the **Certificate revocation list base64 encoded** section, which shows the CRL in base-64 format.
5. Copy the base-64 encoded CRL, including the **-----BEGIN CERTIFICATE REVOCATION LIST-----** and **-----END CERTIFICATE REVOCATION LIST-----** marker lines, to the clipboard or a text file.

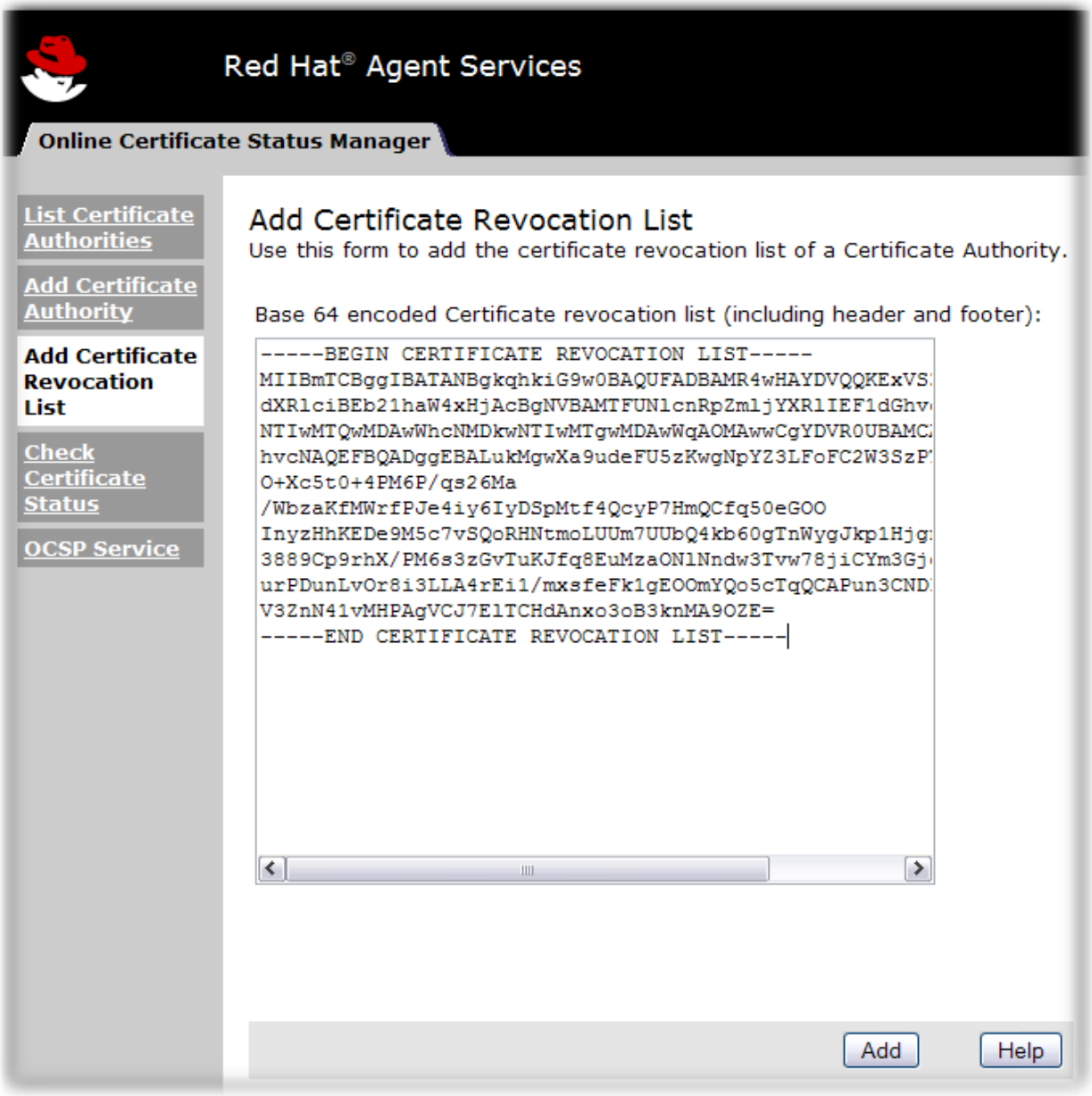
   The CRL looks similar to the example:

   ```
   -----BEGIN CERTIFICATE REVOCATION LIST-----
   MIHiMIGNAgEBMA0GCSqGSIb3DQEBBQUAMEsxGDAWBgNVBAoTD0RvbWFpbiBTcG9v
   bmJveTEPMA0GA1UECxMGMTAyNnNiMR4wHAYDVQQDExVDZXJ0aWZpY2F0ZSBBdXRo
   b3JpdHkXDTA2MTExMzE4MDM0MFoXDTA2MTExMzIyMDM0MFqgDjAMMAoGA1UdFAQD
   AgFeMA0GCSqGSIb3DQEBBQUAA0EAlbdl7bPD5yLpBwKkSXeSA1fa8M2TiqNynRS1
   B5zDGGAamOBdnKVMEBPEXFsTzk92rjbL0J0KjoMYicTEGO1wKA==
   -----END CERTIFICATE REVOCATION LIST-----
   ```

6. Open the Online Certificate Status Manager's agent services page.

   ```
   https://server.example.com:11443/ocsp/agent/ocsp
   ```

7. In the left frame, click **Add Certificate Revocation List**.
8. Paste the encoded CRL inside the **Base 64 encoded certificate revocation list (including the header and footer)** text area.



9. Click **Add**.

   The CRL is added to the internal database of the Online Certificate Status Manager.

8.5. Checking the Revocation Status of a Certificate

The revocation status of a certificate is checked by submitting the certificate in its base-64 encoded format to the Online Certificate Status Manager.

1. Open the Certificate Manager's end-entities page.

```
https://server.example.com:9444/ca/ee/ca
```

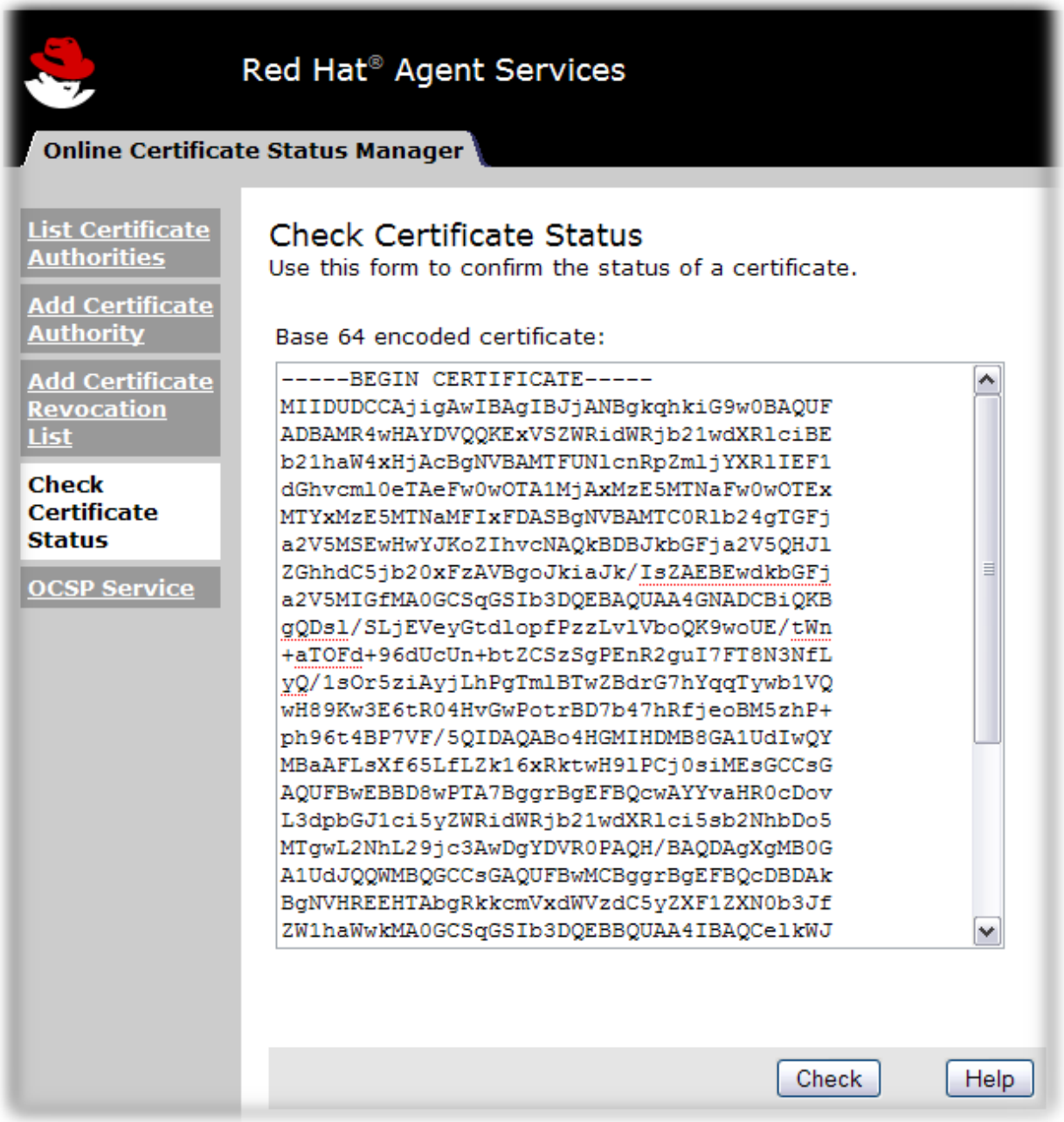
NOTE

The easiest way to get the certificate to verify is to retrieve it from the issuing CA. It is also possible to export it from the client using it, like a browser.

2. Select the **Retrieval** tab, and, in the left frame, click **List Certificates**.
3. When the page opens, click **Find**.
4. Locate the certificate by looking at the subject name of the certificate. This will usually have the server name or user name in the subject name of the certificate.
5. Click on the subject name.
6. In the certificate contents page, scroll to the **Base 64 encoded certificate** section, which shows the CA signing certificate in its base-64 encoded format.
7. Copy the base-64-encoded certificate, including the **-----BEGIN CERTIFICATE-----** and **-----END CERTIFICATE-----** marker lines, to the clipboard or a text file.
8. Open the Online Certificate Status Manager agent services page.

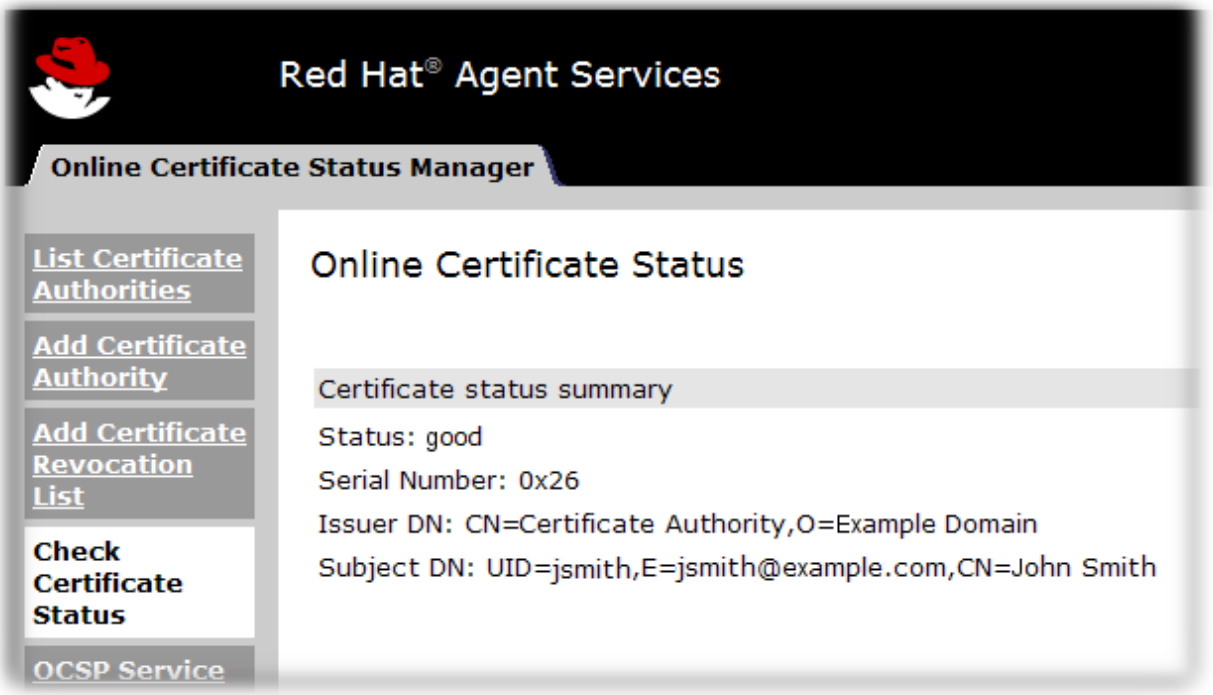
```
https://server.example.com:11443/ocsp/agent/ocsp
```

9. In the left frame, click **Check Certificate Status**.



10. Paste the certificate inside the **Base 64 encoded certificate** text area.

11. Click **Check**.
12. The results page shows the status of the certificate that was submitted.



8.6. OCSP Responder Summary

The Online Certificate Status Manager agent services page also includes a summary of the total processes performed by the subsystem instance, like the total number of OCSP requests and its total processing time since the instance was last started. This is a useful way to track traffic for an OCSP responder and its performance.

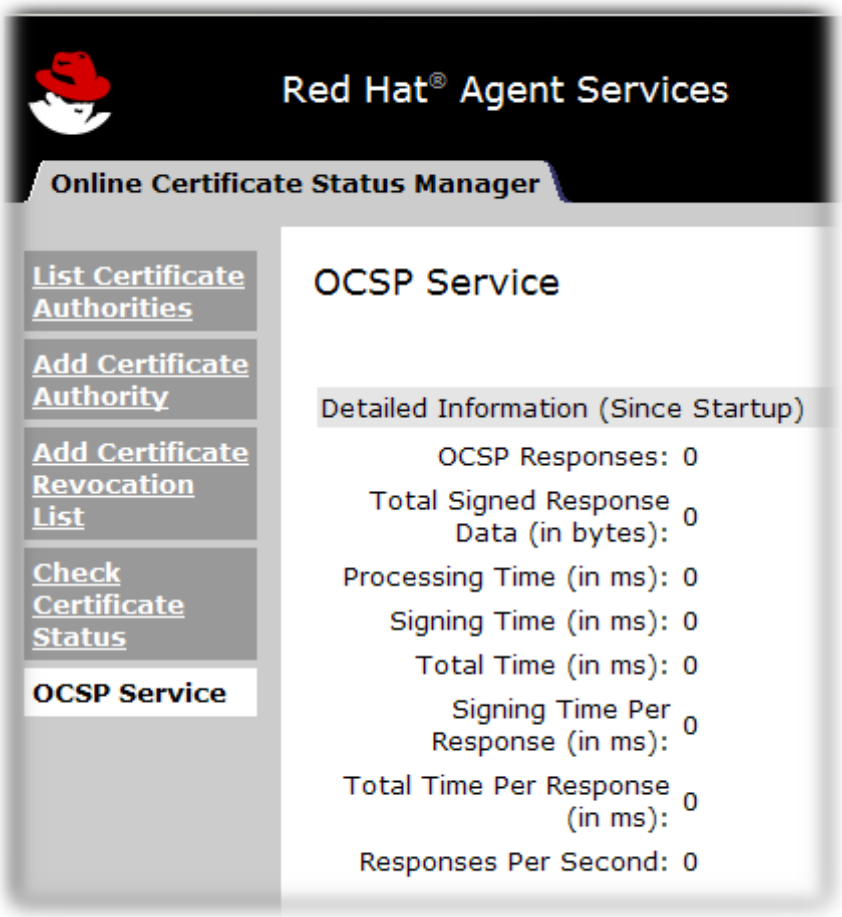

Red Hat® Agent Services
Online Certificate Status Manager
List Certificate Authorities
Add Certificate Authority
Add Certificate Revocation List
Check Certificate Status
OCSP Service
OCSP Service
Detailed Information (Since Startup)
OCSP Responses: 0
Total Signed Response Data (in bytes): 0
Processing Time (in ms): 0
Signing Time (in ms): 0
Total Time (in ms): 0
Signing Time Per Response (in ms): 0
Total Time Per Response (in ms): 0
Responses Per Second: 0

Figure 8.3. OCSP Summary

The signing time is the amount of processing time spent signing responses. The processing time is the time spent verifying the status of the certificate. The total time is the sum of the signing and processing times.

The time per response metrics (signing time and total time) and responses per second metric show the performance of the OCSP responder. Very high response times, lasting several seconds, could indicate that traffic is heavy for the Online Certificate Status Manager or that the configuration of the subsystem or its host server is suboptimal.

Chapter 9. TPS: Managing Token and Smart Card Operations

The Token Processing System (TPS) interacts with the Enterprise Security Client to format tokens, issue certificates on them, and manage the tokens. These tasks are performed by TPS agents using the TPS agent services pages.

The TPS, like the RA, has no separate administrative console; therefore, administrator tasks are also performed through the HTML-based services pages. Additionally, token management can be monitored by people, called operators, who cannot otherwise edit or enroll tokens.

All three TPS roles and their tasks are described in this chapter.

NOTE

Smart cards are also referred to as *tokens* in this chapter and in the TPS services pages.

9.1. Overview of TPS Roles

TPS users are divided into three roles:

- *Agents*, who perform actual token management operations, such as setting the token status, and changing token policies
- *Administrators*, who manage users for the TPS subsystem and have limited control over tokens
- *Operators*, who have no management control but are able to view tokens, certificates, and activities performed through the TPS

Each role's tasks page is accessed through a tab at the top of the TPS pages. A tab is only visible if the user who is logged into the TPS services page belongs to that role. It is possible for a user to belong to more than one role; the default **`admin`** user, for example, belongs to all three roles.

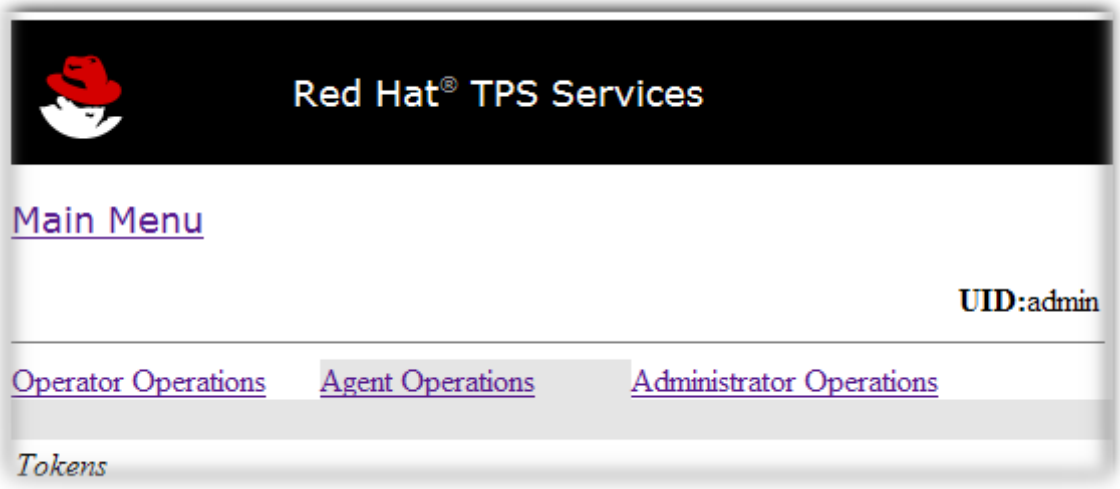


Figure 9.1. TPS Services Menu

NOTE

There is no HTML end entities page for TPS services since end entity tasks are performed through the Enterprise Security Client.

The TPS services pages manage four areas for tokens:

- Tokens
- Certificates issued to tokens
- Activities performed on the TPS, such as creating tokens or users or editing entries, analogous to viewing logs for other subsystems
- TPS subsystem users

Operators can view any token-related entries (meaning tokens, certificates, and activities), but they cannot edit them.

The TPS agents can both view and edit tokens (both for policies and status) and view certificates and activities.

TPS administrators can view tokens and certificates, can add and delete tokens, and can add, edit, and delete TPS users. Administrators can also view slightly more activities than agents or operators because they can view both token and user events.

Each tab is accessed by the roles defined on the user entry and by authenticating to the TPS site with the appropriate certificate.

The information available to each role can be limited to specific enrollment profiles. Enrollment profiles for tokens are similar to the enrollment profiles for CAs; they define a certain use or kind of token enrollment. The default profiles relate to user and security officer enrollments. Custom enrollments can be added.

9.2. Performing Operator Tasks

The **`Operator Operations`** tab has three main areas to search tokens, certificates, and activities.

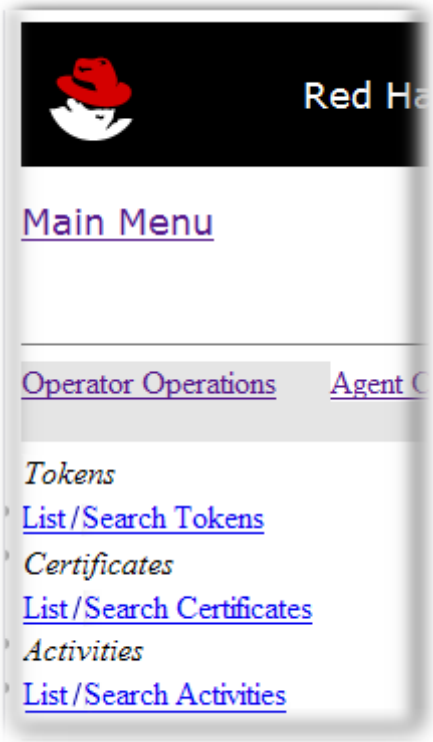


Figure 9.2. Operator Tasks

IMPORTANT

A user can only see entries relating to the profile configured for it. This means that all results are filtered by the profiles that the user can view, including listing and searching for certificates, tokens, or activities.
Setting profiles for users is described in Section 9.4.2.3, “Setting Profiles for Users”.

9.2.1. Searching Tokens

To look for all tokens, a subset of tokens, or a specific token, click the **List/Search Tokens** link, and fill in the name of the user or the whole or partial token identification number (CUID). Asterisks (*****) can be used in the search fields as wildcards. Leaving the field blank returns all tokens.

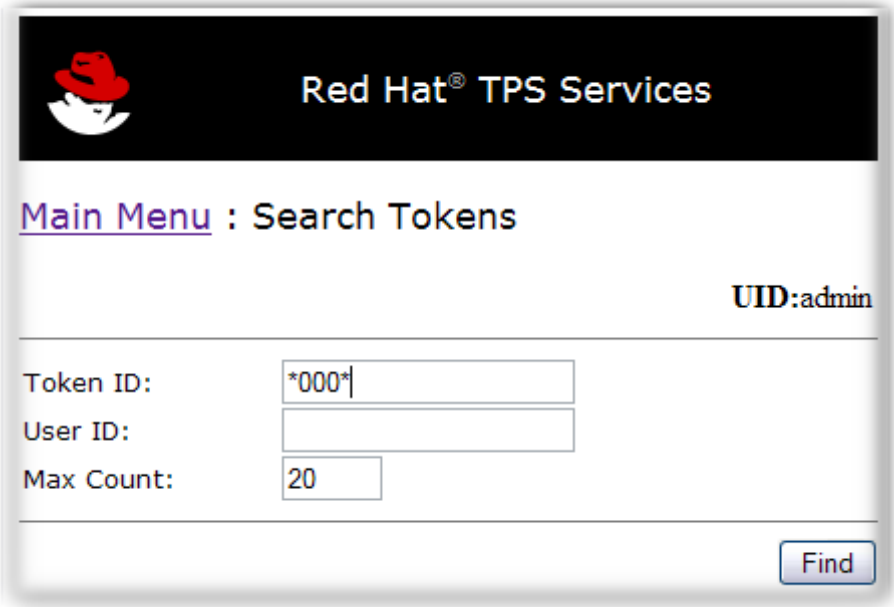


Figure 9.3. Results for Searching for Tokens

There is a maximum allowed number of search results configured for the TPS Directory Server database, so the number of entries returned is constrained by the search limit. Each results page shows 25 records.

9.2.2. Viewing Tokens

After searching for tokens, click the link of the token ID to view the token information.

The token information shows the current definition and state of the token:

- *Token*, the token ID number entered in the TPS.
- *User ID*, user of the token.

- *Status* and *Reason*, the current state of the token.
  - **`uninitialized`** means the token has not been processed
  - **`initialized`** means that the smart card is formatted, but does not have any certificates enrolled on it
  - **`enrolled`** means that certificates have been installed on it
  - **`lost`** or **`onHold`** means it has been suspended, and any suspended or revoked token also has an attribute to show the reason why the token status was changed
- *Policy*, which sets the user policies for the token, such as whether the token can be reused.
- *Token Type*, which is the enrollment profile which is used to enroll the token.

The system information shows information about the token that is processed by the TPS:

- *Key Info*, the types of keys and bit strength generated for the token
- *Applet ID*, the applet loaded on the token
- *Creation Date* and *Modification Date*, which shows the days that the token was first entered in the TPS and the most recent change to the token

Additionally, there are two other sets of information that can be viewed for the token.

- Clicking the **`Show Certificates`** button lists the certificates which are stored on the token.
- Clicking the **`Show Activities`** button lists the operations which have been performed on the token.

9.2.3. Searching Certificates

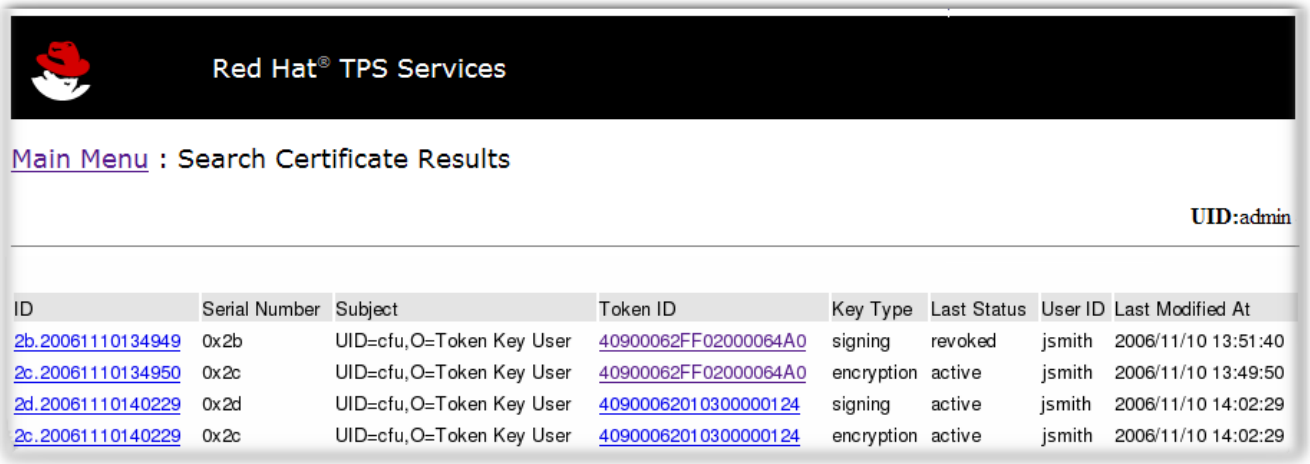
NOTE

It is possible to list the certificates for a single token by opening the token information page and then clicking the **`Show Certificates`** button.

Certificates are recorded as attributes of the token, so the search is for the *token* rather than the certificate alone.

To find all tokens, a subset of tokens, or a specific token, click the **`List/Search Certificates`** link in the **`Operator Operations`** tab, and fill in the name of the user or the whole or partial token identification number (CUID). The certificates search form, then, appears identical to the regular token search form. As with searching for tokens, asterisks (**`*`**) can be used in the search fields as wildcards and leaving a field blank returns all tokens.

There is a maximum allowed number of search results configured for the TPS Directory Server database, so the number of entries returned is constrained by the search limit. Each results page shows 25 records.



ID	Serial Number	Subject	Token ID	Key Type	Last Status	User ID	Last Modified At
2b.20061110134949	0x2b	UID=cfu,O=Token Key User	40900062FF02000064A0	signing	revoked	jsmith	2006/11/10 13:51:40
2c.20061110134950	0x2c	UID=cfu,O=Token Key User	40900062FF02000064A0	encryption	active	jsmith	2006/11/10 13:49:50
2d.20061110140229	0x2d	UID=cfu,O=Token Key User	40900062010300000124	signing	active	jsmith	2006/11/10 14:02:29
2c.20061110140229	0x2c	UID=cfu,O=Token Key User	40900062010300000124	encryption	active	jsmith	2006/11/10 14:02:29

Figure 9.4. Results for Searching for Certificates

The results show all of the information about the certificate:

- *ID*, the unique entry ID for the certificate
- *Serial number*, the serial number of the certificate, which is assigned by the CA which issued it
- *Subject*, the subject name of the certificate; this usually identifies the user of the certificate
- *Token ID*, the ID of the token on which the certificate is enrolled
- *Key Type*, the kind of key, which indicates the purpose or usage of the certificate
- *Last Status*, which is the status of the certificate as of the last time the token was processed (meaning it may not reflect the most current status)
- *User ID*, the user ID of the person who is associated with the token
- *Last Modified At*, the timestamp of the last modification to the certificate

9.2.4. Searching Activities

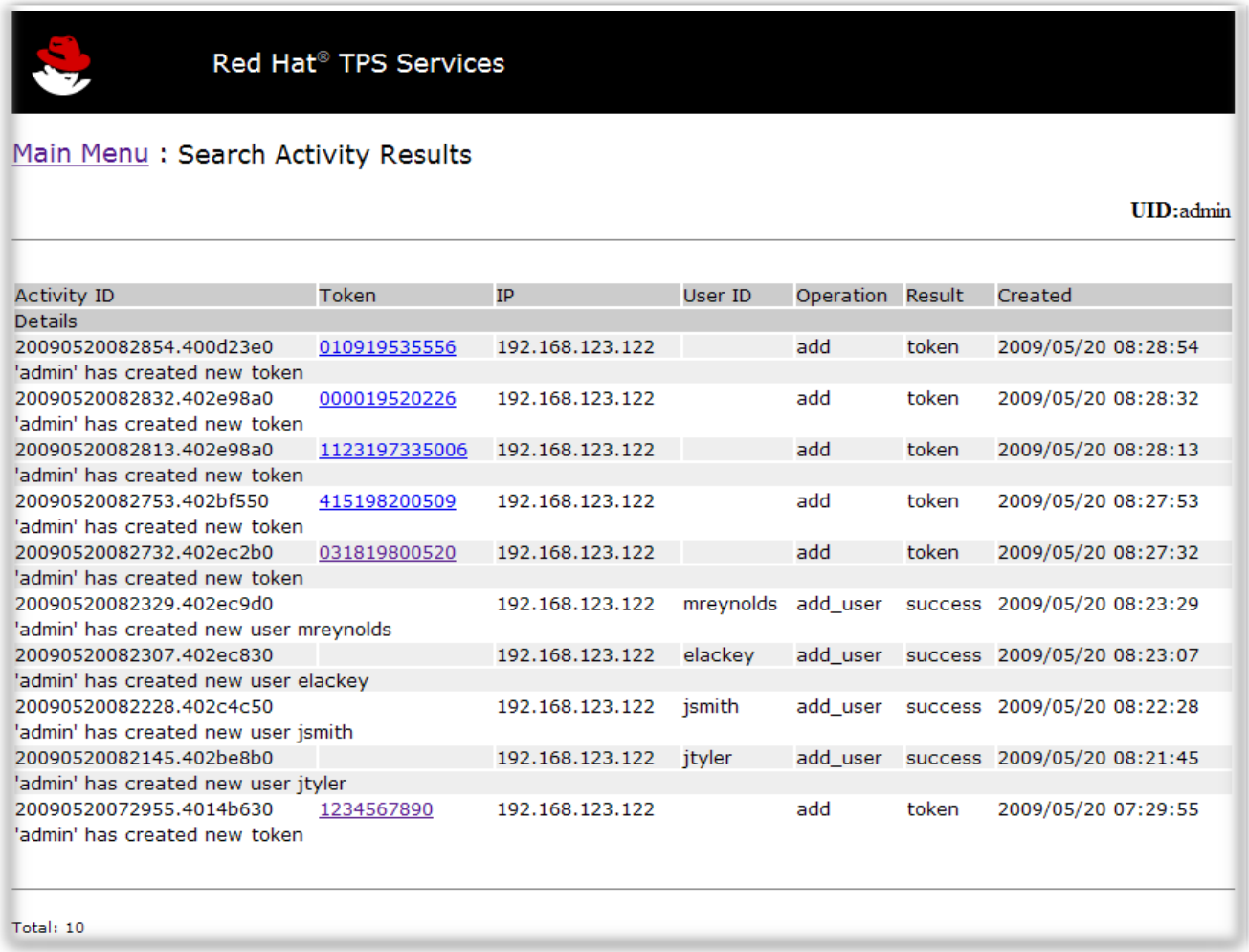
Activities are essentially logs for the TPS subsystem, and for the actions taken on individual tokens.

To find all tokens, a subset of tokens, or a specific token, click the **`List/Search Activities`** link in the **`Operator Operations`** tab, and fill in the name of the user or the whole or partial token identification number (CUID). The certificates search form, then, appears identical to the regular token search form. As with searching for tokens, asterisks (**`*`**) can be used in the search fields as wildcards and leaving a field blank returns all tokens.

There is a maximum allowed number of search results configured for the TPS Directory Server database, so the number of entries returned is constrained by the search limit. Each results page shows 25 records.

NOTE

It is possible to list the activities for a single token by opening the token information page and then clicking the **`Show Activities`** button.



Activity ID	Token	IP	User ID	Operation	Result	Created
Details						
20090520082854.400d23e0	010919535556	192.168.123.122		add	token	2009/05/20 08:28:54
'admin' has created new token						
20090520082832.402e98a0	000019520226	192.168.123.122		add	token	2009/05/20 08:28:32
'admin' has created new token						
20090520082813.402e98a0	1123197335006	192.168.123.122		add	token	2009/05/20 08:28:13
'admin' has created new token						
20090520082753.402bf550	415198200509	192.168.123.122		add	token	2009/05/20 08:27:53
'admin' has created new token						
20090520082732.402ec2b0	031819800520	192.168.123.122		add	token	2009/05/20 08:27:32
'admin' has created new token						
20090520082329.402ec9d0		192.168.123.122	mreynolds	add_user	success	2009/05/20 08:23:29
'admin' has created new user mreynolds						
20090520082307.402ec830		192.168.123.122	elackey	add_user	success	2009/05/20 08:23:07
'admin' has created new user elackey						
20090520082228.402c4c50		192.168.123.122	jsmith	add_user	success	2009/05/20 08:22:28
'admin' has created new user jsmith						
20090520082145.402be8b0		192.168.123.122	jtyler	add_user	success	2009/05/20 08:21:45
'admin' has created new user jtyler						
20090520072955.4014b630	1234567890	192.168.123.122		add	token	2009/05/20 07:29:55
'admin' has created new token						

Figure 9.5. Results for Searching Activities

The activities entries are formatted with two lines of information. The first line has the following information:

- *Activity ID*, the unique ID of the activity entry
- *Token*, the ID of the token for which the activity was performed
- *IP*, the IP address of the client which connected to the TPS and performed the operation
- *User ID*, the ID of the person who performed the operation
- *Operation*, the kind of action being taken
- *Result*, the result returned for the operation
- *Created*, the time that the activity was performed

The second line contains a detailed description of what operation was performed.

9.3. Performing Agent Tasks

Agents perform two important management tasks for tokens: setting the token status and setting the token policies. They can also edit the token information, search certificates, and search activities.

IMPORTANT

A user can only see entries relating to the profile configured for it. This means that all results are filtered by the profiles that the user can view, including listing and searching for certificates, tokens, or activities.
Setting profiles for users is described in Section 9.4.2.3, “Setting Profiles for Users”.

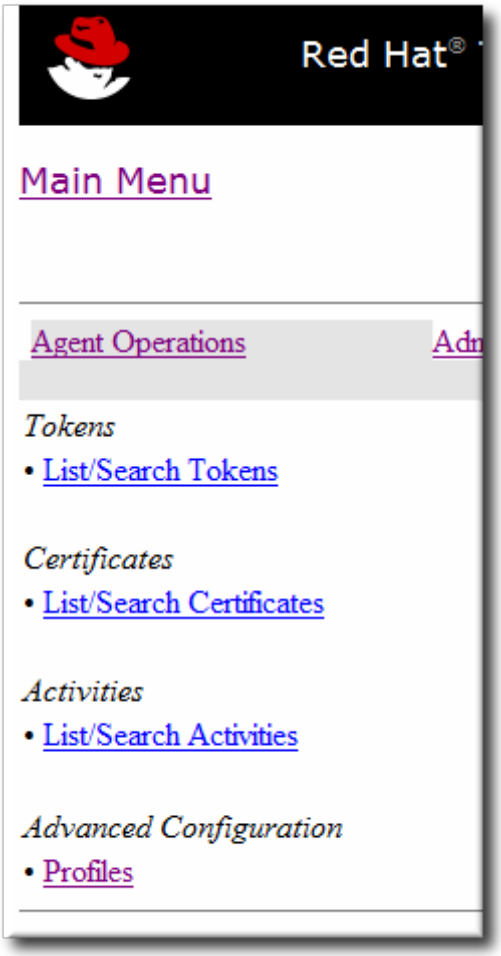


Figure 9.6. Agent Tasks

9.3.1. Searching Tokens

To look for all tokens, a subset of tokens, or a specific token, click the **List/Search Tokens** link, and fill in the name of the user or the whole or partial token identification number (CUID). Asterisks (*****) can be used in the search fields as wildcards.

NOTE

A user can only see entries relating to the profile configured for it, including both token operations and tokens themselves. For an agent to be able to see a certain token or group of tokens, then the agent user entry must be configured to view that token profile.
Setting profiles for users is described in Section 9.4.2.3, “Setting Profiles for Users”.

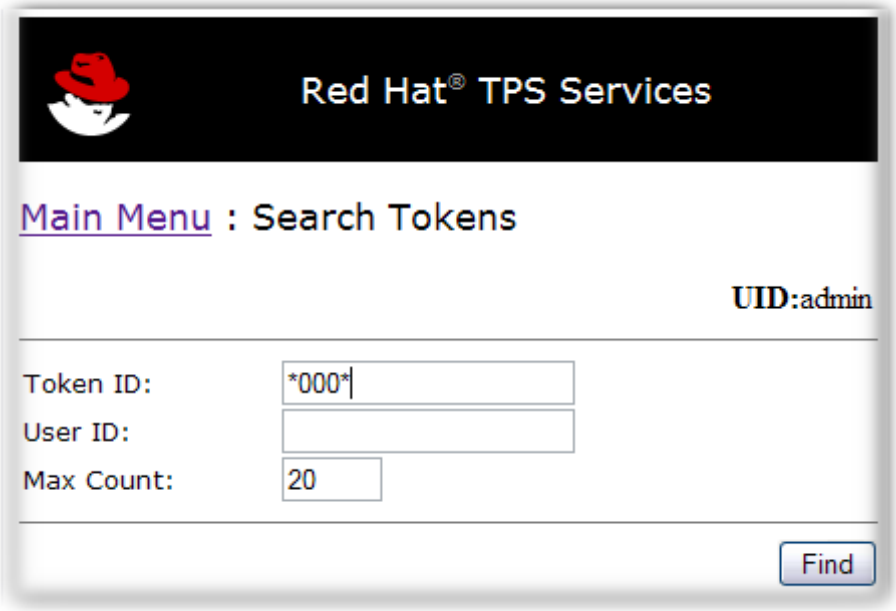


Figure 9.7. Searching for Tokens

There is a maximum allowed number of search results configured for the TPS Directory Server database, so the number of entries returned is constrained by the search limit. Each results page shows 25 records.

9.3.2. Viewing Tokens

After searching for tokens, click the link of the token ID to view the token information.

The token information shows the current definition and state of the token:

- *Token*, the token ID number entered in the TPS.
- *User ID*, user of the token.

- *Status* and *Reason*, the current state of the token.
  - **`uninitialized`** means the token has not been processed
  - **`initialized`** means that the smart card is formatted, but does not have any certificates enrolled on it
  - **`enrolled`** means that certificates have been installed on it
  - **`lost`** or **`onHold`** means it has been suspended, and any suspended or revoked token also has an attribute to show the reason why the token status was changed
- *Policy*, which sets the user policies for the token, such as whether the token can be reused.
- *Token Type*, which is the enrollment profile which is used to enroll the token.

The system information shows information about the token that is processed by the TPS:

- *Key Info*, the types of keys and bit strength generated for the token
- *Applet ID*, the applet loaded on the token
- *Creation Date* and *Modification Date*, which shows the days that the token was first entered in the TPS and the most recent change to the token

Additionally, there are two other sets of information that can be viewed for the token.

- Clicking the **`Show Certificates`** button lists the certificates which are stored on the token.
- Clicking the **`Show Activities`** button lists the operations which have been performed on the token.

The agent can also edit the token, as described in Section 9.3.3, “Managing Tokens”.

9.3.3. Managing Tokens

When viewing a token, an agent can edit the token information, change the token status, and set policies for the token.

NOTE

A user can only see entries relating to the profile configured for it, including both token operations and tokens themselves. For an agent to be able to see a certain token or group of tokens, then the agent user entry must be configured to view that token profile.
Setting profiles for users is described in Section 9.4.2.3, “Setting Profiles for Users”.

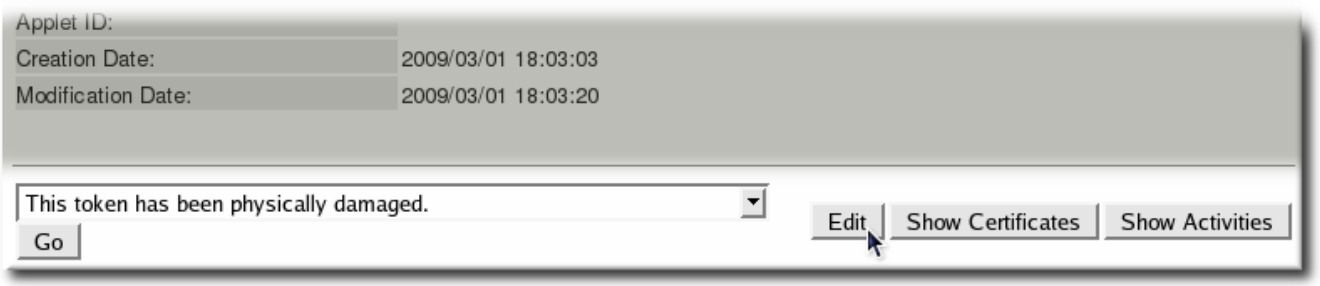


Figure 9.8. Managing Tokens

9.3.3.1. Editing the Token Information

At the bottom of the token information screen, there is an **Edit** button. Two fields can be edited for the token: the user name of the user with whom the token is associated and the token policy.

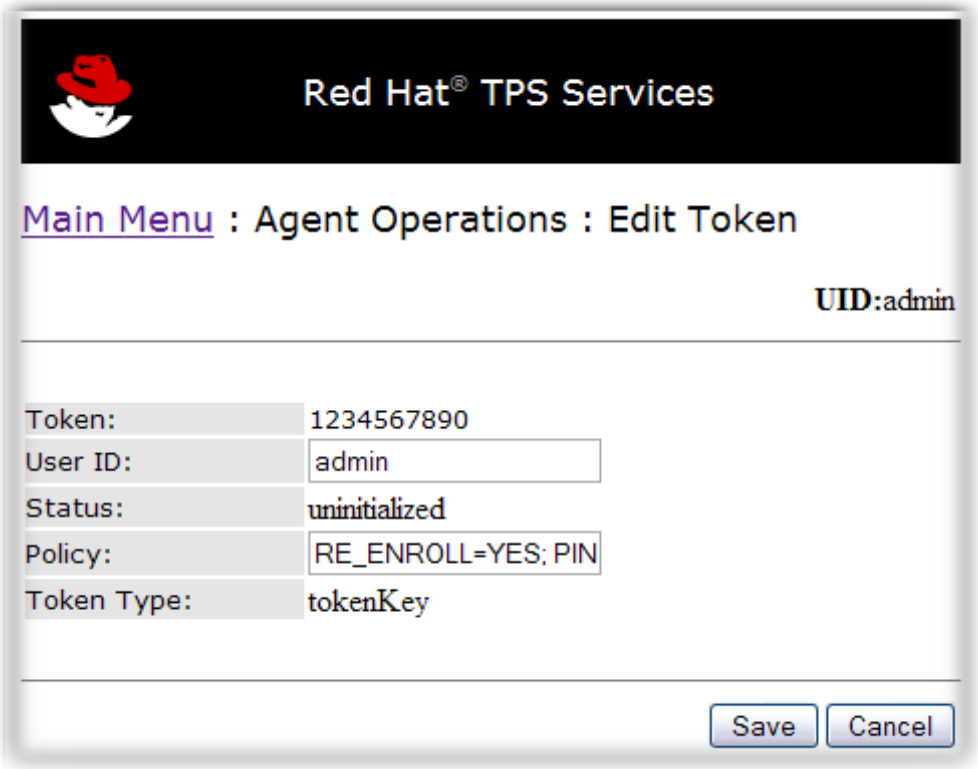


Figure 9.9. Editing the Token Information

9.3.3.2. Changing the Token Policy

The policy sets rules on what the user can do after the token is enrolled.

There are four supported token policies:

- **RE_ENROLL**, which allows a user to re-enroll certificates with the same token
- **PIN_RESET**, which allows the token user to initiate a PIN reset operation
- **RENEW**, which allows a user to regenerate their existing certificates using the original key and an extended validity period
- **FORCE_FORMAT**, which causes every enrollment operation to prompt a format operation. This is a last-step option to allow tokens to be reset without a user having to return it to an administrator.

IMPORTANT

If this policy is set, then this should be the only token policy configured. This takes precedence over any other policy.

The supported token policies accept values of either **YES** or **NO**. To set both policies, separate them with a semi-colon. For example:

```
RE_ENROLL=NO;PIN_RESET=YES
```

The default values is for the **RE_ENROLL** and **PIN_RESET** parameters to be set to **YES**.

If both **RE_ENROLL** and **RENEW** are set to **YES**, then the renewal setting takes precedence, the token certificates are renewed when they expire.

NOTE

If the **PIN_RESET** policy is not set, then user-initiated PIN resets are allowed by default. If the policy is present and is changed from **NO** to **YES**, then a PIN reset can be initiated by the user once; after the PIN is reset, the policy value automatically changes back to **NO**.

To edit the policy settings, search for the token, and click its ID link.

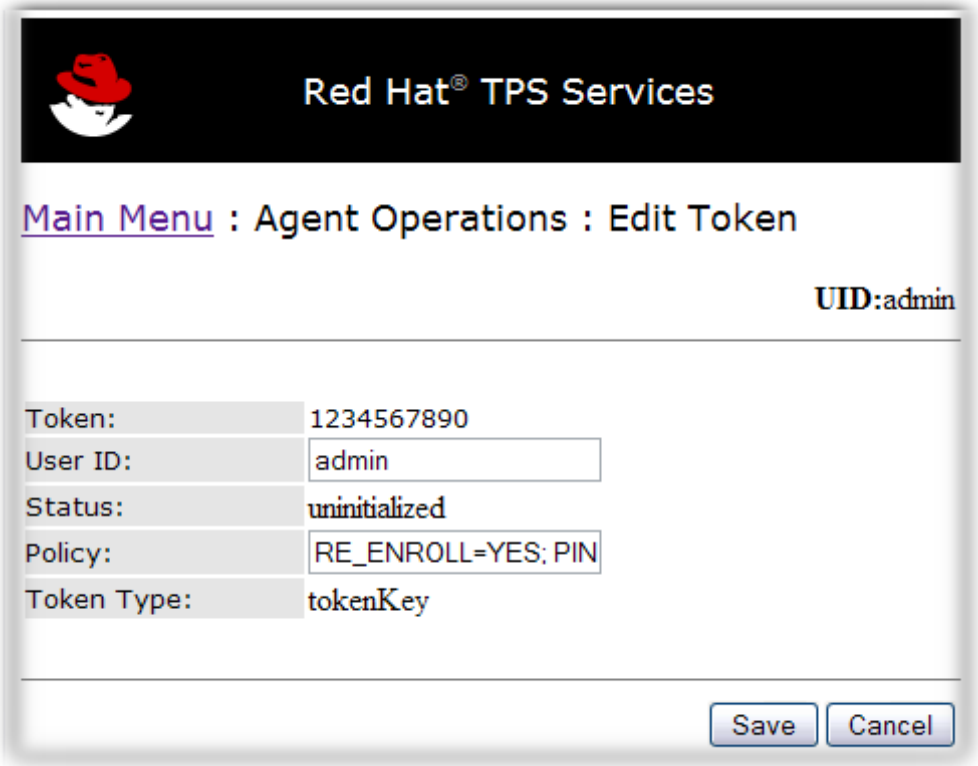


Figure 9.10. Editing the Token Policy

9.3.3.3. Changing Token Status

Agents can change the status of the token. Token status affects key recovery policies; the status of the token impacts whether a key should be recovered from the DRM or reissued, whether new tokens will be blocked because there are already active existing tokens, and whether to issue or revoke temporary tokens.

The status is changed through the token details page, which is shown by searching for tokens and then selecting a token from the returned list.

To change the status, select the menu item, and click **Go**.

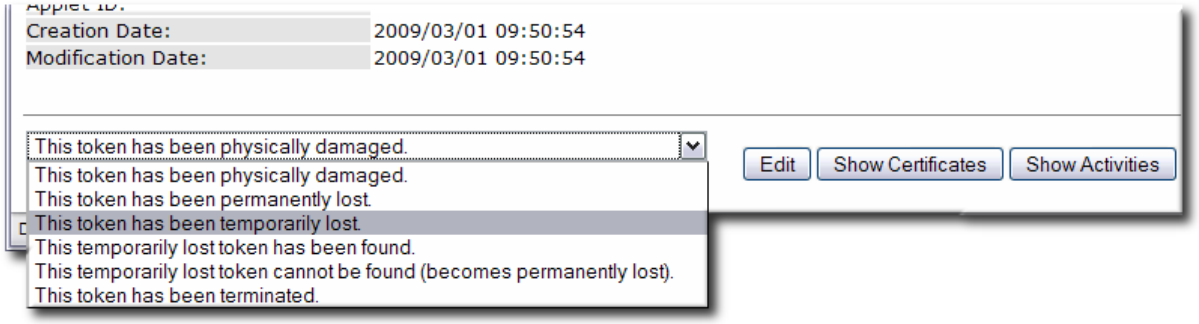

Creation Date:
2009/03/01 09:50:54
Modification Date:
2009/03/01 09:50:54
This token has been physically damaged.
This token has been physically damaged.
This token has been permanently lost.
This token has been temporarily lost.
This temporarily lost token has been found.
This temporarily lost token cannot be found (becomes permanently lost).
This token has been terminated.
Edit
Show Certificates
Show Activities

Figure 9.11. Changing Status

There are six possible token statuses. A status is only active in the drop-down menu of the transition from the current status is allowed. For example, a token should not logically be allowed to move from a permanently lost status to a found status, so this option is grayed out in the menu.

NOTE

Moving from one status to another is a *transition*. Only certain transitions are allowed; for example, an administrator can block a token that is marked as permanently lost from ever being marked again as active. The allowed token transitions are set by an administrator in the TPS's **`CS.cfg`** file in the ***`tokendb.allowedTransitions`*** parameter. For information on setting status transitions for tokens, see the *Administrator's Guide*.

Table 9.1. Token Statuses

Status	Meaning	Action
The token is physically damaged.	The TPS revokes the user certificates and marks the token lost.	The original certificates are revoked, and new certificates for the user can be generated on a new token.
The token has been permanently lost.	The TPS revokes the user certificates and marks the token lost.	The original certificates are revoked, and new certificates for the user can be generated on a new token.
The token is temporarily lost or unavailable.	The TPS puts the user certificates on hold and marks the token inactive.	The original certificates are suspended and put on hold (meaning they cannot be used until the status changes). New, temporary certificates for the user can be generated on a new token.
The lost token has been found.	The TPS takes the certificates off hold and marks the token active.	The temporary certificates are revoked, and the original certificates are taken off hold.
The lost token cannot be found (permanently lost).	The TPS revokes the certificates and marks the token lost.	The temporary certificates and the original certificates are revoked, and new certificates for the user can be generated on a new token.
This token has been terminated.	The TPS terminates the token. Terminating a token terminates the certificates and keys on the token and breaks the association between the token and the user in the token database. The physical token can still be formatted and reused afterward, but this change of status will mark a record of the termination event.	The original certificates are revoked. The token itself can be reused and enrolled for new users or certificates.

Changing the status of the token to anything other than active has two possible actions. If the token is permanently taken offline (permanently lost, damaged, or terminated), then the certificates on the token are revoked and the token is inactivated. However, if the token is temporarily lost or inaccessible, then the token is essentially suspended, the certificates on it are inactivated, and a new token with temporary certificates is issued.

NOTE

If a token is terminated, the physical token can be reused with new certificates.

Temporary certificates, by default, are only valid for one week. Within that time, the status on the original token has to be finalized, in one of two ways:

- The token could be found. If the user locates the original token, the TPS agent can reactivate the original token by changing the status to **`This temporarily lost token has been found`**. Changing the status of the original token to active also takes the certificates off hold; when this is done, the status of the temporary token is automatically updated and its certificates revoked.
- If the user cannot locate the original token, the TPS agent must change the status of the original token to **`This temporarily lost token cannot be found`**. The certificates on the original token are revoked. The status of the temporary token is updated to inactive and its certificates revoked. The user is then permitted to enroll for a permanent token.

9.3.4. Searching Certificates

NOTE

It is possible to list the certificates for a single token by opening the token information page and then clicking the **`Show Certificates`** button.

Certificates are recorded as attributes of the token, so the search is for the *token* rather than the certificate alone.

To find all tokens, a subset of tokens, or a specific token, click the **`List/Search Certificates`** link in the **`Agent Operations`** tab, and fill in the name of the user or the whole or partial token identification number (CUID). The certificates search form, then, appears identical to the regular token search form. As with searching for tokens, asterisks (**`*`**) can be used in the search fields as wildcards and leaving a field blank returns all tokens.

There is a maximum allowed number of search results configured for the TPS Directory Server database, so the number of entries returned is constrained by the search limit. Each results page shows 25 records.

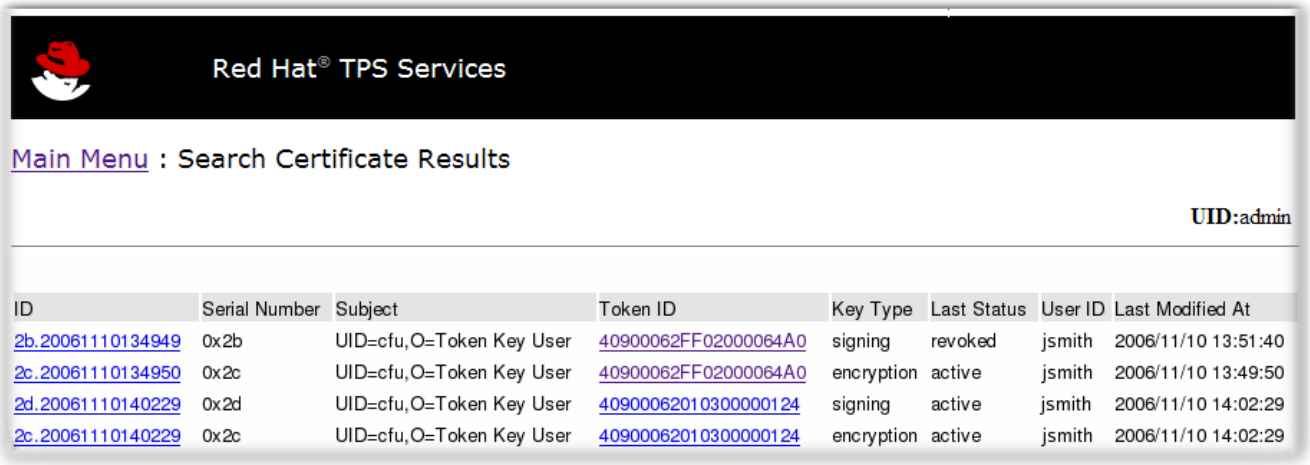

Red Hat® TPS Services
Main Menu : Search Certificate Results
UID:admin
ID Serial Number Subject Token ID Key Type Last Status User ID Last Modified At
2b.20061110134949 0x2b UID=cfu,O=Token Key User 40900062FF02000064A0 signing revoked jsmith 2006/11/10 13:51:40
2c.20061110134950 0x2c UID=cfu,O=Token Key User 40900062FF02000064A0 encryption active jsmith 2006/11/10 13:49:50
2d.20061110140229 0x2d UID=cfu,O=Token Key User 40900062010300000124 signing active jsmith 2006/11/10 14:02:29
2c.20061110140229 0x2c UID=cfu,O=Token Key User 40900062010300000124 encryption active jsmith 2006/11/10 14:02:29

Figure 9.12. Results for Searching for Certificates

The results show all of the information about the certificate:

- *ID*, the unique entry ID for the certificate
- *Serial number*, the serial number of the certificate, which is assigned by the CA which issued it
- *Subject*, the subject name of the certificate; this usually identifies the user of the certificate

- *Token ID*, the ID of the token on which the certificate is enrolled
- *Key Type*, the kind of key, which indicates the purpose or usage of the certificate
- *Last Status*, which is the status of the certificate as of the last time the token was processed (meaning it may not reflect the most current status)
- *User ID*, the user ID of the person who is associated with the token
- *Last Modified At*, the timestamp of the last modification to the certificate

9.3.5. Searching Activities

Activities are essentially logs for the TPS subsystem, and for the actions taken on individual tokens.

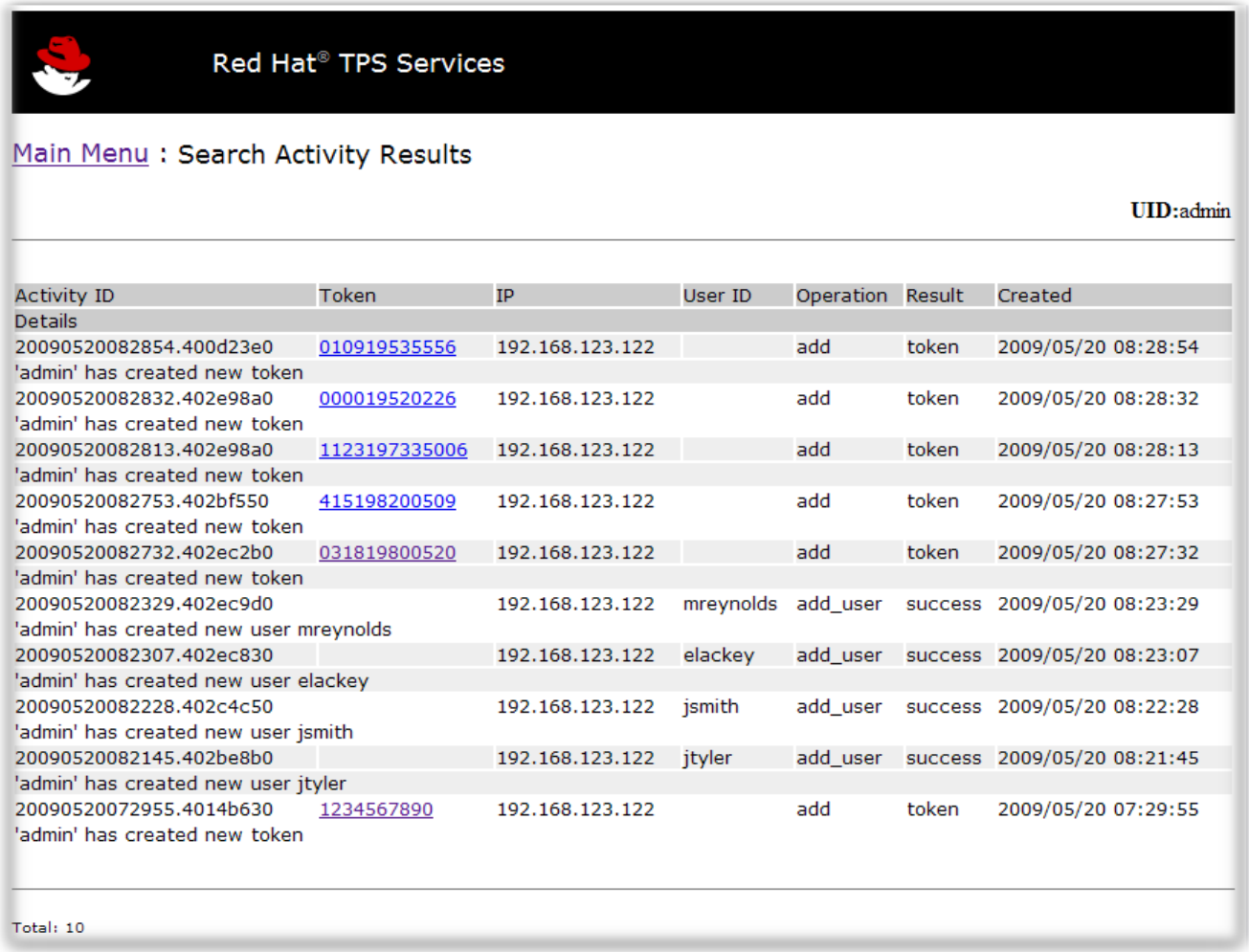
Activities are logs of actions performed on a token, so searching for activities means searching for the token, and returning its specific log of activities.

To find all tokens, a subset of tokens, or a specific token, click the **`List/Search Activities`** link in the **`Agent Operations`** tab, and fill in the name of the user or the whole or partial token identification number (CUID). The certificates search form, then, appears identical to the regular token search form. As with searching for tokens, asterisks (**`*`**) can be used in the search fields as wildcards and leaving a field blank returns all tokens.

NOTE

It is possible to list the activities for a single token by opening the token information page and then clicking the **`Show Activities`** button.

There is a maximum allowed number of search results configured for the TPS Directory Server database, so the number of entries returned is constrained by the search limit. Each results page shows 25 records.



Red Hat® TPS Services

Main Menu : Search Activity Results

UID:admin

Activity ID	Token	IP	User ID	Operation	Result	Created
Details						
20090520082854.400d23e0	010919535556	192.168.123.122		add	token	2009/05/20 08:28:54
'admin' has created new token						
20090520082832.402e98a0	000019520226	192.168.123.122		add	token	2009/05/20 08:28:32
'admin' has created new token						
20090520082813.402e98a0	1123197335006	192.168.123.122		add	token	2009/05/20 08:28:13
'admin' has created new token						
20090520082753.402bf550	415198200509	192.168.123.122		add	token	2009/05/20 08:27:53
'admin' has created new token						
20090520082732.402ec2b0	031819800520	192.168.123.122		add	token	2009/05/20 08:27:32
'admin' has created new token						
20090520082329.402ec9d0		192.168.123.122	mreynolds	add_user	success	2009/05/20 08:23:29
'admin' has created new user mreynolds						
20090520082307.402ec830		192.168.123.122	elackey	add_user	success	2009/05/20 08:23:07
'admin' has created new user elackey						
20090520082228.402c4c50		192.168.123.122	jsmith	add_user	success	2009/05/20 08:22:28
'admin' has created new user jsmith						
20090520082145.402be8b0		192.168.123.122	jtyler	add_user	success	2009/05/20 08:21:45
'admin' has created new user jtyler						
20090520072955.4014b630	1234567890	192.168.123.122		add	token	2009/05/20 07:29:55
'admin' has created new token						

Total: 10

Figure 9.13. Results for Searching Activities

The activities entries are formatted with two lines of information. The first line has the following information:

- *Activity ID*, the unique ID of the activity entry
- *Token*, the ID of the token for which the activity was performed
- *IP*, the IP address of the client which connected to the TPS and performed the operation
- *User ID*, the ID of the person who performed the operation
- *Operation*, the kind of action being taken
- *Result*, the result returned for the operation
- *Created*, the time that the activity was performed

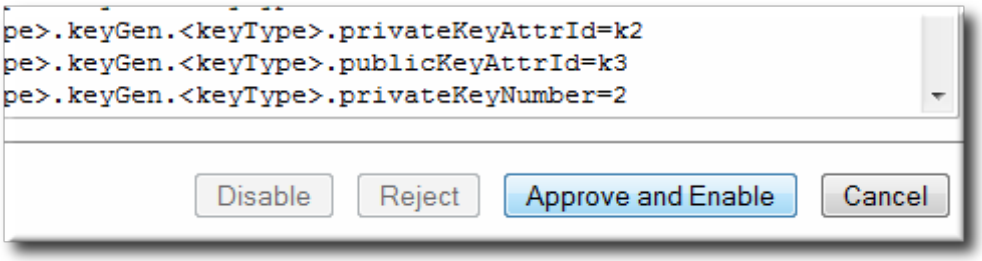
The second line contains a detailed description of what operation was performed.

9.3.6. Enabling and Disabling Profiles

Similar to a CA profile, the TPS uses profiles to define the policies for its token operations. These policies are created and edited by TPS administrators, but they must be reviewed and enabled by TPS agents.

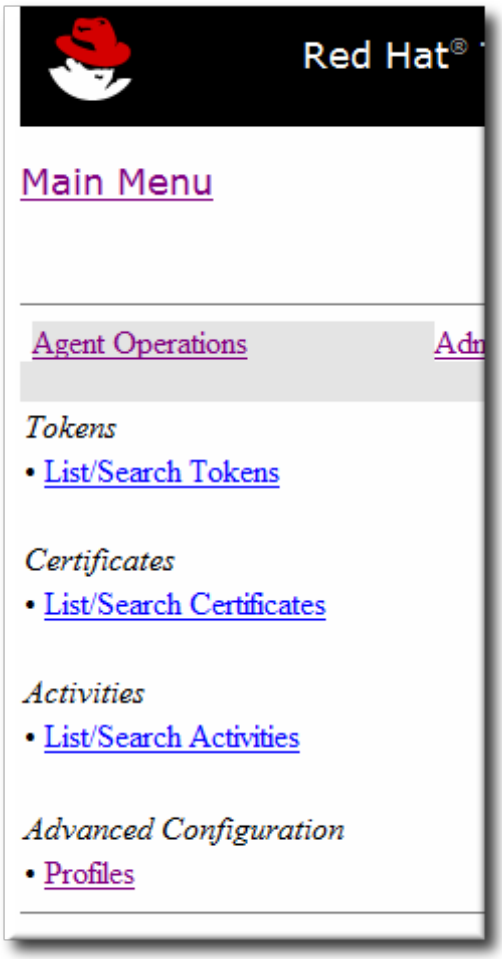
9.3.6.1. Enabling Profiles

1. Click the **Profiles** link in the **Agents Operations** tab.
2. Select the policy from the drop-down menu and click the **Review** button.
3. Review the edited profile, and click the **Approve and Enable** button at the bottom of the screen.

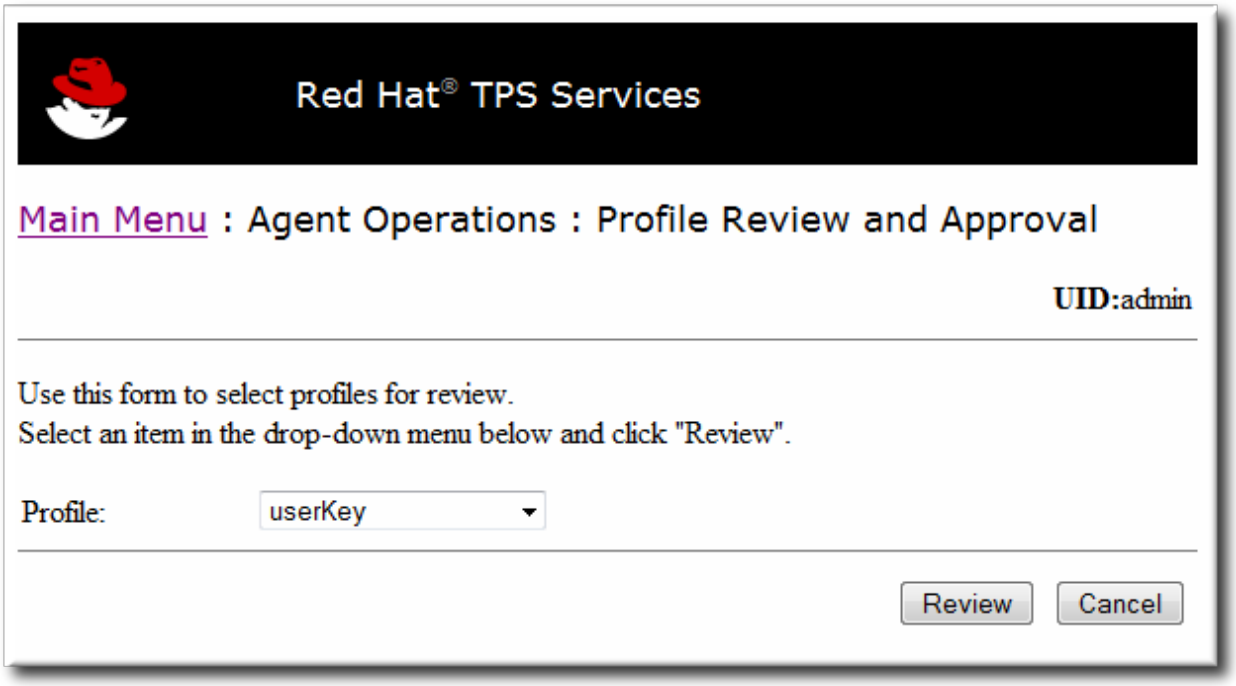


9.3.6.2. Disabling Profiles

1. Click the **Profiles** link in the **Agents Operations** tab.



2. Select the policy from the drop-down menu and click the **Review** button.


Red Hat® TPS Services
Main Menu : Agent Operations : Profile Review and Approval
UID:admin
Use this form to select profiles for review.
Select an item in the drop-down menu below and click "Review".
Profile:
userKey
Review
Cancel

3. At the bottom of the policy page, click the **`Disable`** button.

9.4. Performing Administrator Tasks

An administrator maintains the server configuration in the internal database and the token database.

- Adding and deleting tokens manually in the token database
- Creating and editing users for the TPS subsystem
- Managing audit logging for the TPS instance
- Running and configuring self-tests
- Editing and creating TPS profiles and profile mappings
- Setting up LDAP authentication sources
- Adding subsystem connections
- Setting general server configuration, including secure channels and search parameters

An administrator can also perform common tasks, like viewing tokens and activity logs.

IMPORTANT

A user can only see entries relating to the profile configured for it. This means that all results are filtered by the profiles that the user can view, including listing and searching for certificates, tokens, or activities. For an administrator to be able to manage all tokens, then the user account needs to be set to **`All profiles`**.
Setting profiles for users is described in Section 9.4.2.3, “Setting Profiles for Users”.

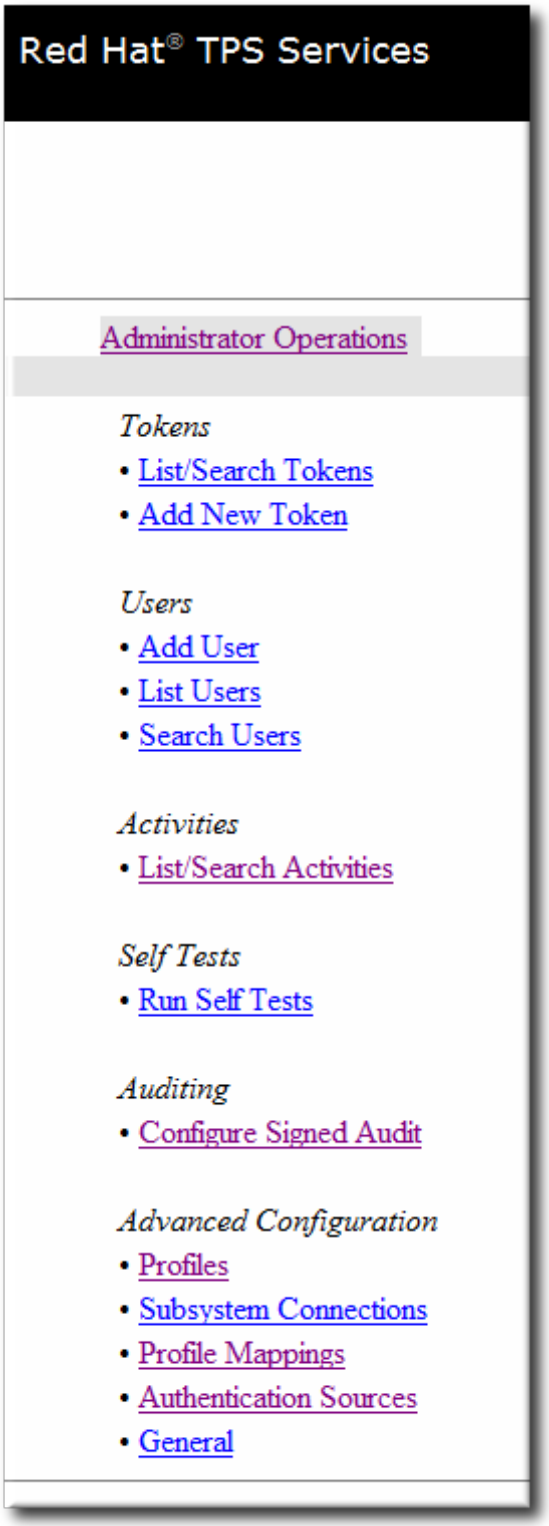


Figure 9.14. Administrator Tasks

9.4.1. Managing Tokens

Administrators cannot manage token *information* the way that agents can, but they can manually create or delete token entries from the token database, the repository which the TPS uses to identify and manage tokens.

9.4.1.1. Adding Tokens

New tokens are added to the TPS subsystem through the **Add tokens** link in the **Admin Operations** tab. The only required information is the token ID, which is embedded in the token. Additional information about the token can be added through the agent edit page.

Normally, it is not necessary to create a token entry because the entry is created automatically when the token connects to TPS, such as connecting through the Enterprise Security Client. However, it may be necessary to pre-populate the tokens with keys or other custom information; this can be done by manually adding and editing the token in the TPS.

9.4.1.2. Searching Tokens

To look for all tokens, a subset of tokens, or a specific token, click the **List/Search Tokens** link, and fill in the name of the user or the whole or partial token identification number (CUID). Asterisks (*****) can be used in the search fields as wildcards.

NOTE

A user can only see entries relating to the profile configured for it, including both token operations and tokens themselves. For an administrator to be able to search and manage all tokens configured in the TPS, the administrator user entry should be set to **All profiles**. Setting profiles for users is described in Section 9.4.2.3, “Setting Profiles for Users”.

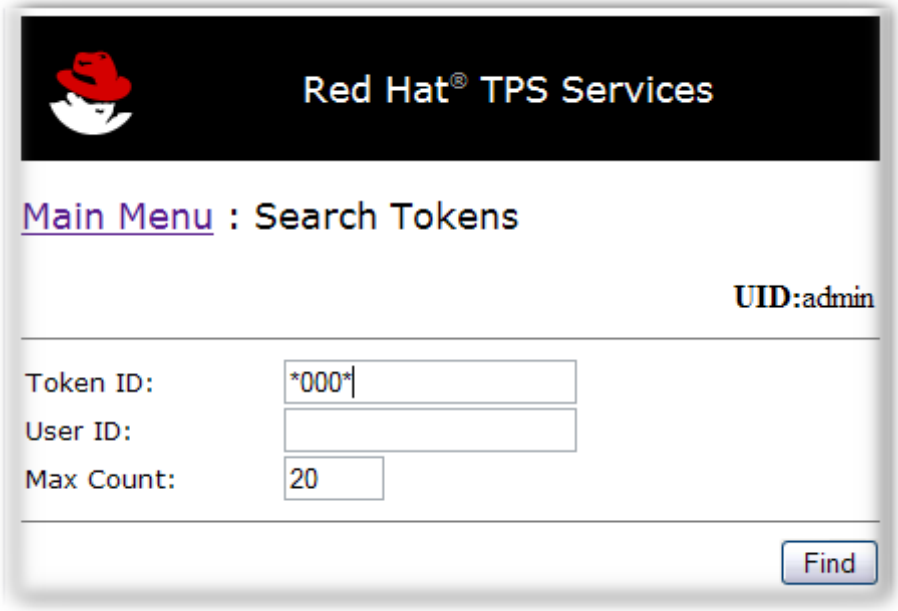


Figure 9.15. Searching for Tokens

There is a maximum allowed number of search results configured for the TPS Directory Server database, so the number of entries returned is constrained by the search limit. Each results page shows 25 records.

9.4.1.3. Viewing Tokens

After searching for tokens, click the link of the token ID to view the token information.

Token Information:

Token:	098765654
User ID:	jsmith
Status:	uninitialized
Reason:	
Policy:	RE_ENROLL=YES
Token Type:	tokenKey

System Information:

Key Info:	
Applet ID:	
Creation Date:	2009/03/01 18:03:03
Modification Date:	2009/03/01 18:03:20

The token information shows the current definition and state of the token:

- *Token*, the token ID number entered in the TPS.
- *User ID*, user of the token.
- *Status* and *Reason*, the current state of the token.
  - **`uninitialized`** means the token has not been processed
  - **`initialized`** means that the smart card is formatted, but does not have any certificates enrolled on it
  - **`enrolled`** means that certificates have been installed on it
  - **`lost`** or **`onHold`** means it has been suspended, and any suspended or revoked token also has an attribute to show the reason why the token status was changed
- *Policy*, which sets the user policies for the token, such as whether the token can be reused.
- *Token Type*, which is the enrollment profile which is used to enroll the token.

The system information shows information about the token that is processed by the TPS:

- *Key Info*, the types of keys and bit strength generated for the token
- *Applet ID*, the applet loaded on the token
- *Creation Date* and *Modification Date*, which shows the days that the token was first entered in the TPS and the most recent change to the token

Additionally, there are two other sets of information that can be viewed for the token.

- Clicking the **`Show Certificates`** button lists the certificates which are stored on the token.
- Clicking the **`Show Activities`** button lists the operations which have been performed on the token.

9.4.1.4. Deleting the Token

1. Search for the token, and click its ID link.
2. Click **`Delete`** in the lower right of the edit page to remove the token, and all its associated certificates and user information, from the TPS database.

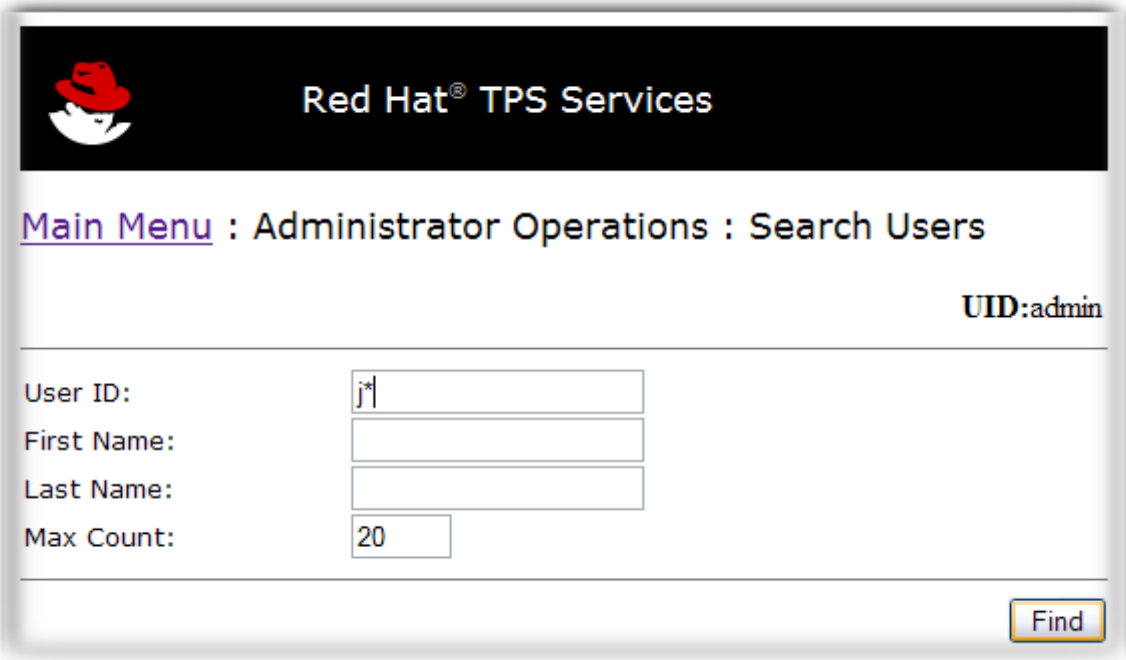
9.4.2. Managing TPS Users

For the TPS subsystem, users are added and managed through the **Administrator Operations** page, which replaces an administrative console for that subsystem.

As with other subsystems, the TPS administrator can create other users who access the TPS subsystem. These users are created through the administrator services tab.

9.4.2.1. Searching Users

Search for all users, a subset of users, or specific users by their subsystem user ID, first name, or last name through the **Search Users** link in the **Administrator Operations** page.



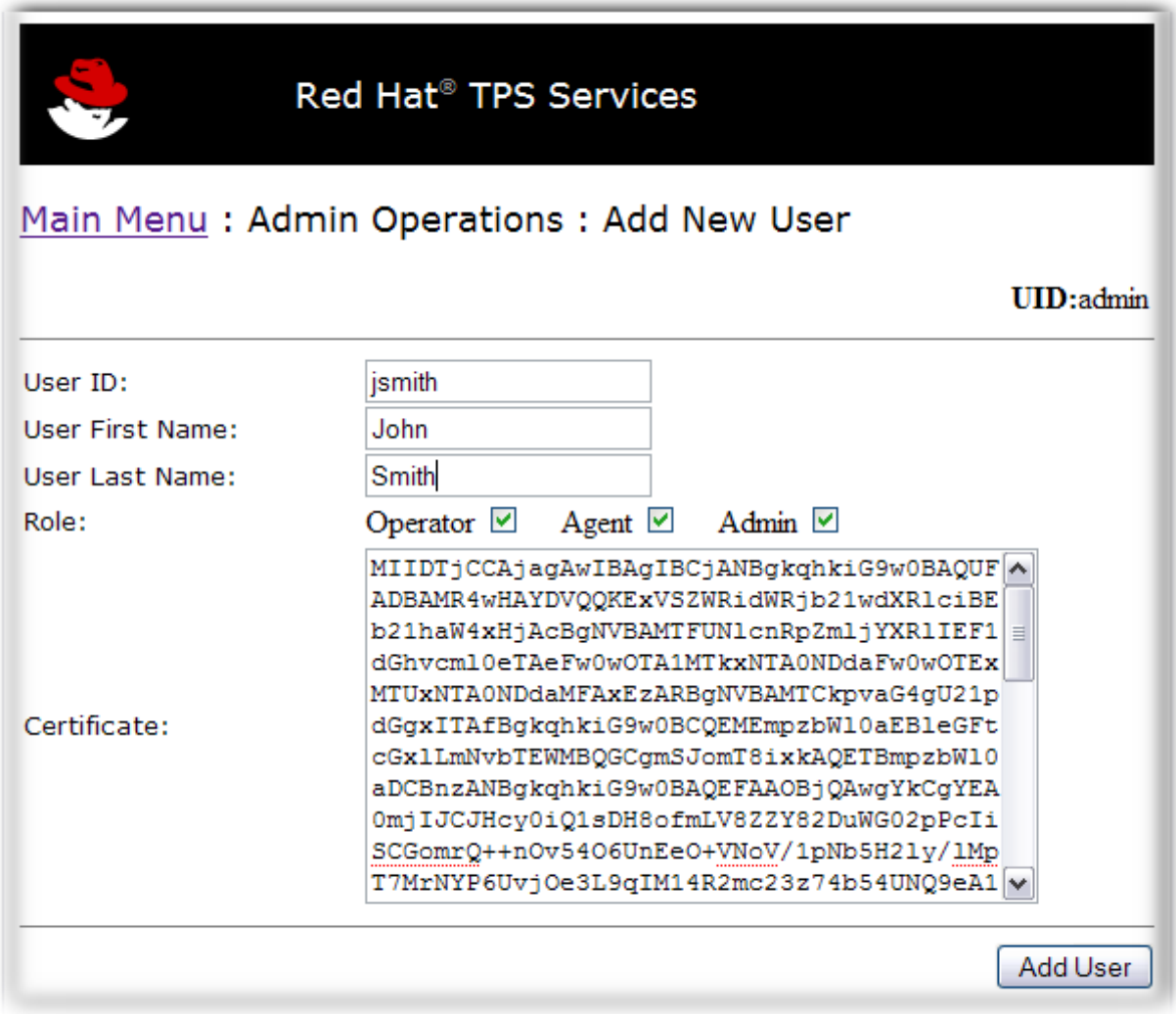
9.4.2.2. Adding Users

1. Obtain a user certificate for the new user. Requesting and submitting certificates is explained in the *End User's Guide*.

   IMPORTANT

   A TPS administrator must have a signing certificate. The recommended profile to use is Manual User Signing and Encryption Certificates Enrollment.

2. Click the **Add New User** link in the **Administrator Operations** tab.
3. Fill in the user's name and ID and paste in the certificate, without the **BEGIN CERTIFICATE** and **END CERTIFICATE** lines.



4. Select the roles to which the user belongs. The user can only see the tabs (services pages) of the roles to which he belongs.

9.4.2.3. Setting Profiles for Users

A TPS profile is much like a CA profile; it defines rules for processing different types of tokens. The profile is assigned automatically to a token based on some characteristic of the token, like the CUID. Users can only see tokens for the profiles which are assigned to them.

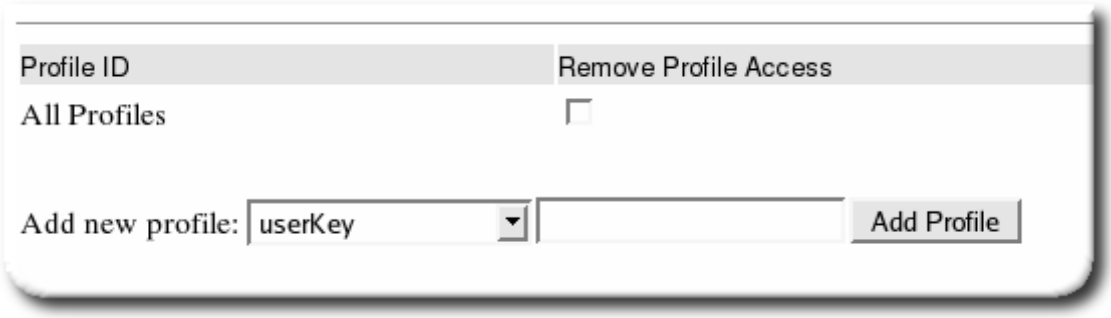
NOTE

A user can only see entries relating to the profile configured for it, including both token operations and tokens themselves. For an administrator to be able to search and manage all tokens configured in the TPS, the administrator user entry should be set to **`All profiles`**. Setting specific profiles for users is a simple way to control access for operators and agents to specific users or token types.

Token profiles are sets of policies and configurations that are applied to a token. Token profiles are mapped to tokens automatically based on some kind of attribute in the token itself, such as a CCUID range. Token profiles are created as other certificate profiles (as in Section 2.1, “About Certificate Profiles”). Configuring token mapping is covered in the *Certificate System Administrator's Guide*.

1. Search for the users, and click the link of the user's name in the results page.

2. Scroll to the bottom of the page, and select the profile from the drop-down menu.



Only fifteen (15) profiles are listed in the menu; if there are more than fifteen profiles available, then the last profile is **Other**, which allows the administrator to type in the selected profile manually.

NOTE

If the **All Profiles** option is added to the user, then any other configured profiles are dropped, because they are already included in the **All Profiles** option.

3. Click the **Add Profile** button to add the profile to the user entry.

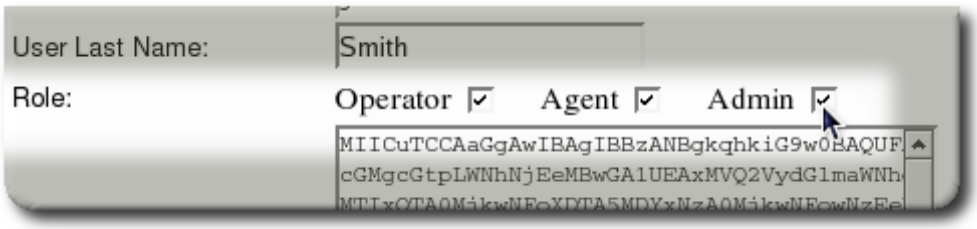
The new profile is listed as part of the user entry attributes. Up to fifteen profiles are listed on the profile; if there are more than fifteen, then the profile list is paginated.

9.4.2.4. Changing Roles for Users

A role is just a group within the TPS. Each role can view different tabs of the TPS services pages. The role is editable, so it is possible to add and remove role assignments for a user.

A user can belong to more than one role. The default admin user, for example, belongs to all three roles.

1. Search for the users, and click the link of the user's name in the results page.
2. Near the top of the page is a series of check boxes for the different roles, **Operator**, **Agent**, and **Administrator**. Check the boxes to assign the roles.



3. Click the **Update** button to save the new role settings.

9.4.2.5. Deleting Users

WARNING

It is possible to delete the *last* user account, and the operation cannot be undone. Be very careful about the user which is selected to be deleted.

1. Search for the user, and click the link to the user to delete.
2. Click the **Delete** button in the lower right of the edit page.

9.4.3. Searching Activities

Activities are essentially logs for the TPS subsystem, and for the actions taken on individual tokens. Administrators can see all of the activities for tokens and certificates that agents and operators see. They can also see non-token operations, like adding or editing users.

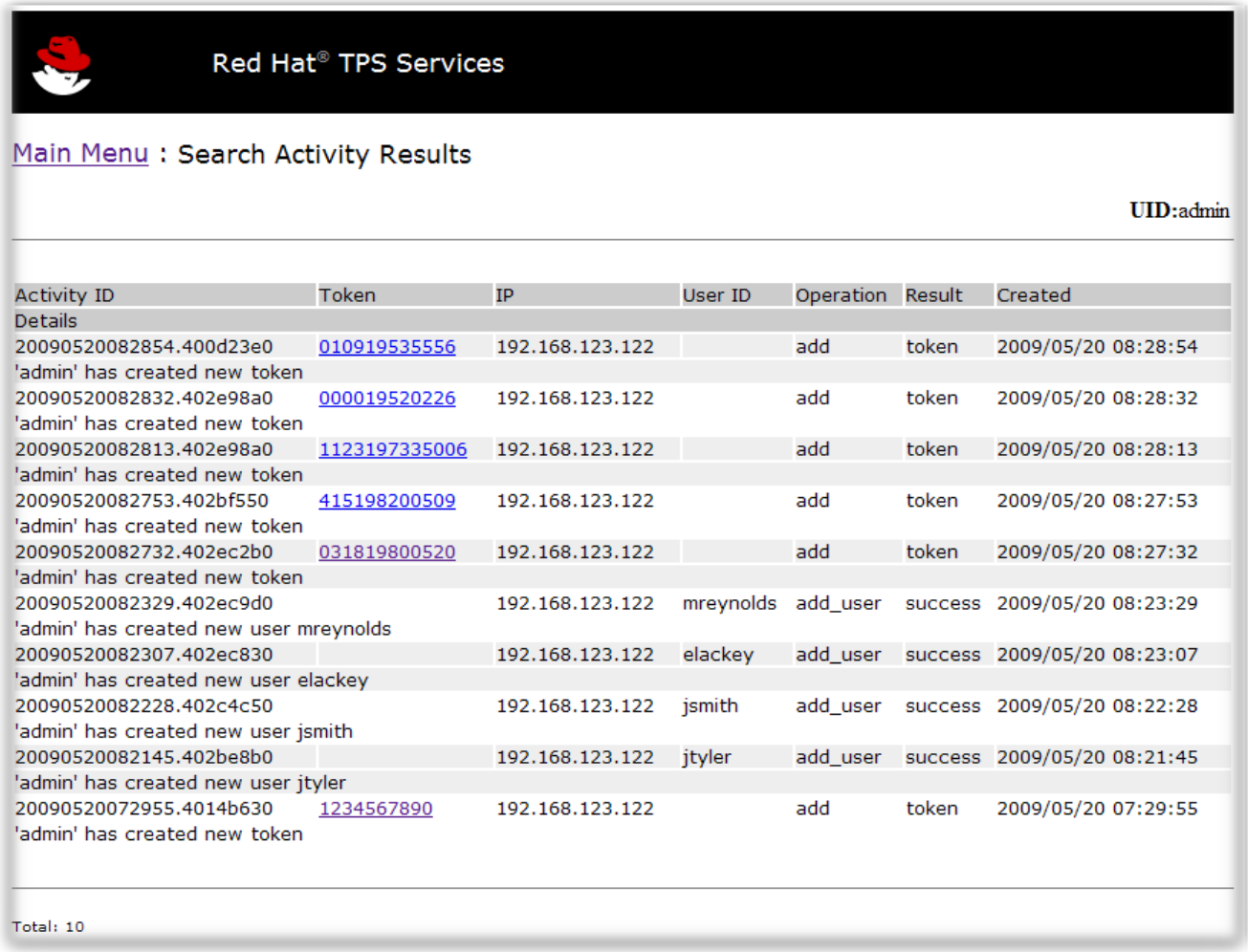
Activities are logs of actions performed on a token, so searching for activities means searching for the token, and returning its specific log of activities.

To find all tokens, a subset of tokens, or a specific token, click the **`List/Search Activities`** link in the **`Administrator Operations`** tab, and fill in the name of the user or the whole or partial token identification number (CUID). The certificates search form, then, appears identical to the regular token search form. As with searching for tokens, asterisks (**`*`**) can be used in the search fields as wildcards and leaving a field blank returns all tokens.

NOTE

It is possible to list the activities for a single token by opening the token information page and then clicking the **`Show Activities`** button.

There is a maximum allowed number of search results configured for the TPS Directory Server database, so the number of entries returned is constrained by the search limit. Each results page shows 25 records.



Red Hat® TPS Services

Main Menu : Search Activity Results

UID:admin

Activity ID	Token	IP	User ID	Operation	Result	Created
Details						
20090520082854.400d23e0	010919535556	192.168.123.122		add	token	2009/05/20 08:28:54
'admin' has created new token						
20090520082832.402e98a0	000019520226	192.168.123.122		add	token	2009/05/20 08:28:32
'admin' has created new token						
20090520082813.402e98a0	1123197335006	192.168.123.122		add	token	2009/05/20 08:28:13
'admin' has created new token						
20090520082753.402bf550	415198200509	192.168.123.122		add	token	2009/05/20 08:27:53
'admin' has created new token						
20090520082732.402ec2b0	031819800520	192.168.123.122		add	token	2009/05/20 08:27:32
'admin' has created new token						
20090520082329.402ec9d0		192.168.123.122	mreynolds	add_user	success	2009/05/20 08:23:29
'admin' has created new user mreynolds						
20090520082307.402ec830		192.168.123.122	elackey	add_user	success	2009/05/20 08:23:07
'admin' has created new user elackey						
20090520082228.402c4c50		192.168.123.122	jsmith	add_user	success	2009/05/20 08:22:28
'admin' has created new user jsmith						
20090520082145.402be8b0		192.168.123.122	jtyler	add_user	success	2009/05/20 08:21:45
'admin' has created new user jtyler						
20090520072955.4014b630	1234567890	192.168.123.122		add	token	2009/05/20 07:29:55
'admin' has created new token						

Total: 10

Figure 9.16. Results for Searching Activities

The activities entries are formatted with two lines of information. The first line has the following information:

- *Activity ID*, the unique ID of the activity entry
- *Token*, the ID of the token for which the activity was performed
- *IP*, the IP address of the client which connected to the TPS and performed the operation
- *User ID*, the ID of the person who performed the operation
- *Operation*, the kind of action being taken (a type of **no_token** means it is an administrative operation)
- *Result*, the result returned for the operation
- *Created*, the time that the activity was performed

The second line contains a detailed description of what operation was performed.

9.4.4. Running Self-Tests

On-demand self-test for the TPS subsystem are run through the **Run Self Tests** link in the **Administrator Operations** page.

The tests that will be run are shown on the **Run Self Tests** page.

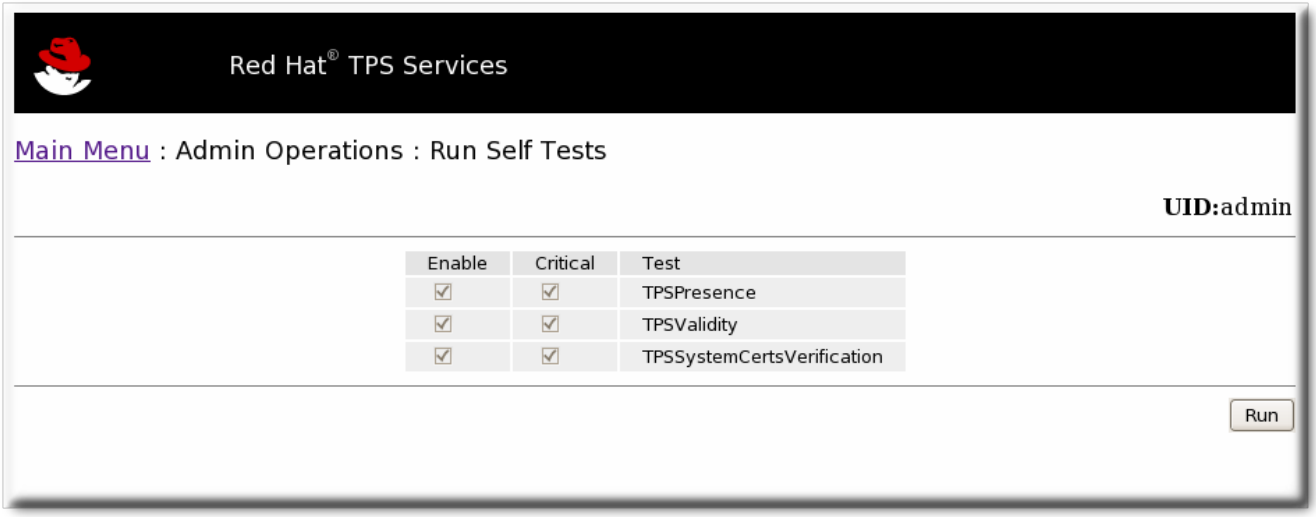


Figure 9.17. Self-Tests

The **TPS Services** page will show the logged events for the self-tests. If any critical self-tests fail, the server will stop.

9.4.5. Managing the TPS Audit Logs

Audit logs are special, protected logs that are used by auditors to track operations in the subsystem, such as for routine security checks or in case of some kind of security breach. Audit logs record a specific, configurable subset of operations.

TPS audit log settings are managed by clicking the **Configuring Signed Audit Logging** link in the **Administrator Operations** tab.

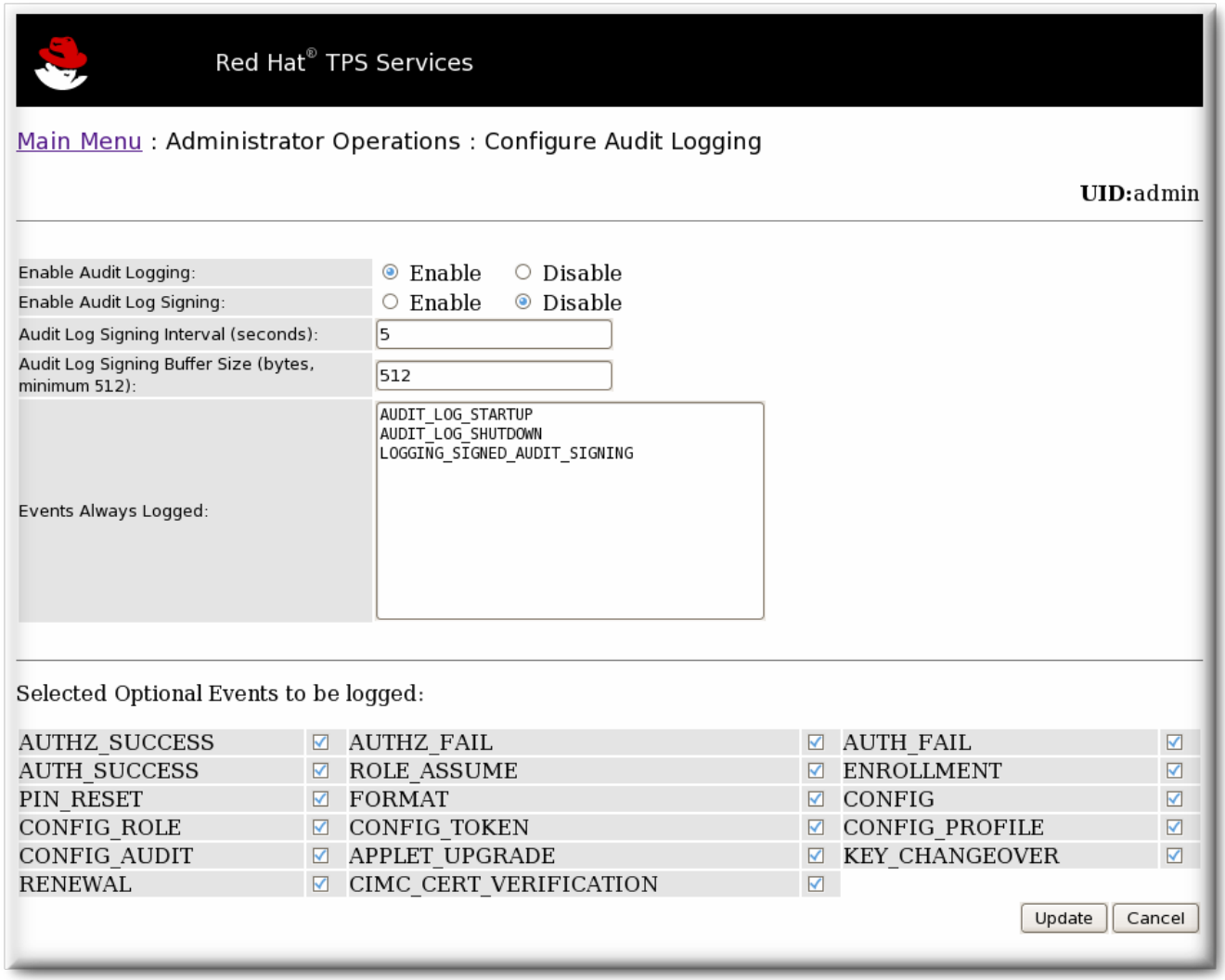


Figure 9.18. Configuring TPS Audit Logging

Audit logs are stored with the other subsystem logs in **`/var/log/`*`subsystem_name`*** (by default). Signed audit logs are written to **`/var/log/`*`subsystem_name`*`/signedAudit`**.

NOTE

For other Certificate System subsystems, audit logging is maintained in the Java-based administrative console. The TPS subsystem, however, does not use a Java console, so administrative tasks are either performed by directly editing the configuration files or, as with managing users, through the administrative page in TPS web services.

There are two parts for enabling audit logging. The first is enabling the audit log itself, using the **`Enable|Disable`** radio buttons. The second part is enabling *signed* audit logging. This signs the audit log after every entry with a special signing certificate as a sign that the log has not been tampered with.

By default, the audit log is enabled, and audit log signing is disabled. After enabling logging, then administrators can set what operations are recorded in the audit log. The loggable events are listed in Table 9.2, “Events Recorded to the TPS Audit Log”, and logging for these events can be added or removed from the audit log settings.

Specifying a value in the **Audit Log Signing Interval** field controls how frequently the server flushes the buffer and writes the messages to the logs. The default value is **5** seconds. Specifying a value in the **Audit Log Signing Buffer Size** field sets the maximum size of the buffer in bytes. The default value is 512 bytes. The buffer will be flushed and the data written to the logs, when the signing interval has expired or the buffer is full.

Table 9.2. Events Recorded to the TPS Audit Log

Event	Description
AUDIT_LOG_STARTUP	The start of the subsystem, and thus the start of the audit function.
AUDIT_LOG_SHUTDOWN	The shutdown of the subsystem, and thus the shutdown of the audit function.
LOGGING_SIGNED_AUDIT_SIGNING	Shows changes in whether the audit log is signed.
AUTHZ_SUCCESS	Shows when a user is successfully processed by the authorization servlets.
AUTH_SUCCESS	Shows when a user successfully authenticates.
ENROLLMENT	Shows when a token is enrolled through the TPS.
APPLET_UPGRADE	Shows when the applet on the token is upgraded.
AUTHZ_FAIL	Shows when a user is not successfully processed by the authorization servlets.
ROLE_ASSUME	A user assuming a role. A user assumes a role after passing through authentication and authorization systems. Only the default roles of administrator, auditor, and agent are tracked. Custom roles are not tracked.
PIN_RESET	Shows when the password used to access the token is reset.
CONFIG	Shows general configuration changes not specifically define below.
CONFIG_ROLE	Shows that a change has been made to the configuration settings for roles, including changes made to users or groups.
CONFIG_TOKEN	Shows that a change was made to a token's configuration settings.
CONFIG_PROFILE	Shows that a change was made to a profile's configuration settings.
CONFIG_AUDIT	Shows that a change was made to the audit log configuration.
KEY_CHANGEOVER	Shows whether key changeover worked successfully.
RENEWAL	Shows if a token is renewed successfully through the TPS.
AUTH_FAIL	Shows when a user does not successfully authenticate.
FORMAT	Records when a token is formatted.
CIMC_CERT_VERIFICATION	Shows when a router (Cisco Integrated Management Controller) certificate verification request has been processed.

9.4.6. Managing TPS Server Configuration

The **`Advanced Configuration`** area of the TPS administrative UI shows different areas that can be

configured specifically relating to the TPS server, such as subsystem connections, LDAP authentication sources, and both operation profiles and profile/smart card mappings. These are all sections in the TPS **CS.cfg** file that are explicitly exposed in the UI for editing or adding entries.

Defining the configuration elements that are manageable in the TPS web services pages is also set in the **CS.cfg** file. This is covered in the *Certificate System Administrator's Guide*.

The advanced configuration areas in the UI simply exposes excerpts from the **CS.cfg** file, without providing guided editable fields or configuration wizards. Editing TPS configuration in the TPS admin UI offers several distinct advantages over editing the **CS.cfg** file directly:

- The TPS UI provides a visual list of changes, displaying both additions and deletions.
- The TPS UI validates the format of the parameters used in the configuration.
- Every configuration change is automatically recorded to the TPS audit logs. Whenever a new entry is added or an entry is edited, the change is recorded with the configuration area and entry name, plus the timestamp and the change that was made.

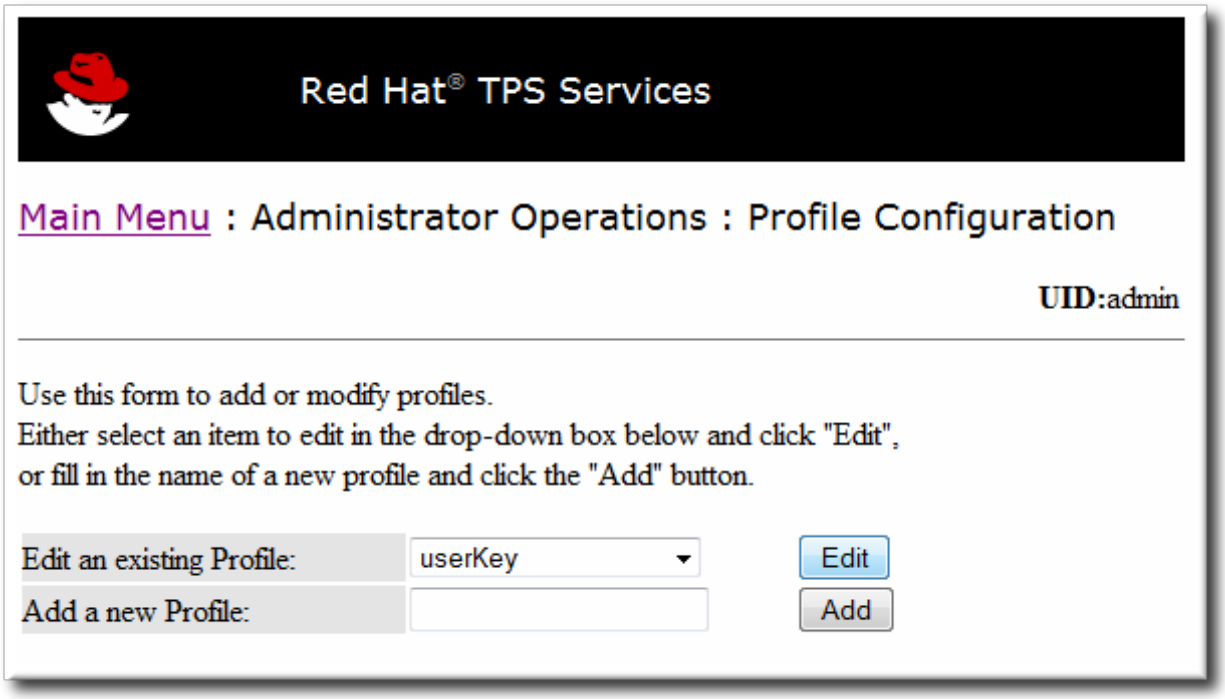
9.4.6.1. Editing TPS Profiles

The TPS profiles are configured based on the token operation.

NOTE

A profile must be disabled by an agent before it can be edited, and then it must be re-enabled by an agent before it can be used.

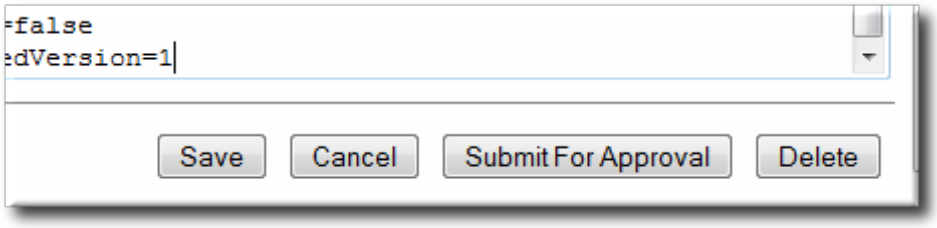
1. In the **Administrator Operations** tab, click the **Profiles** link.
2. Select the profile from the drop-down menu and click the **Edit** button.


Red Hat® TPS Services
Main Menu : Administrator Operations : Profile Configuration
UID:admin
Use this form to add or modify profiles.
Either select an item to edit in the drop-down box below and click "Edit",
or fill in the name of a new profile and click the "Add" button.
Edit an existing Profile:
userKey
Edit
Add a new Profile:
Add

3. Edit the profile as desired. The parameters for the profiles is covered in the *Certificate System Administrator's Guide*.
4. Click the **Submit for Approval** button to send the edited profile back to the agent for approval. Submitting the profile for approval locks the configuration so that it cannot be changed

until an agent either accepts or rejects it.

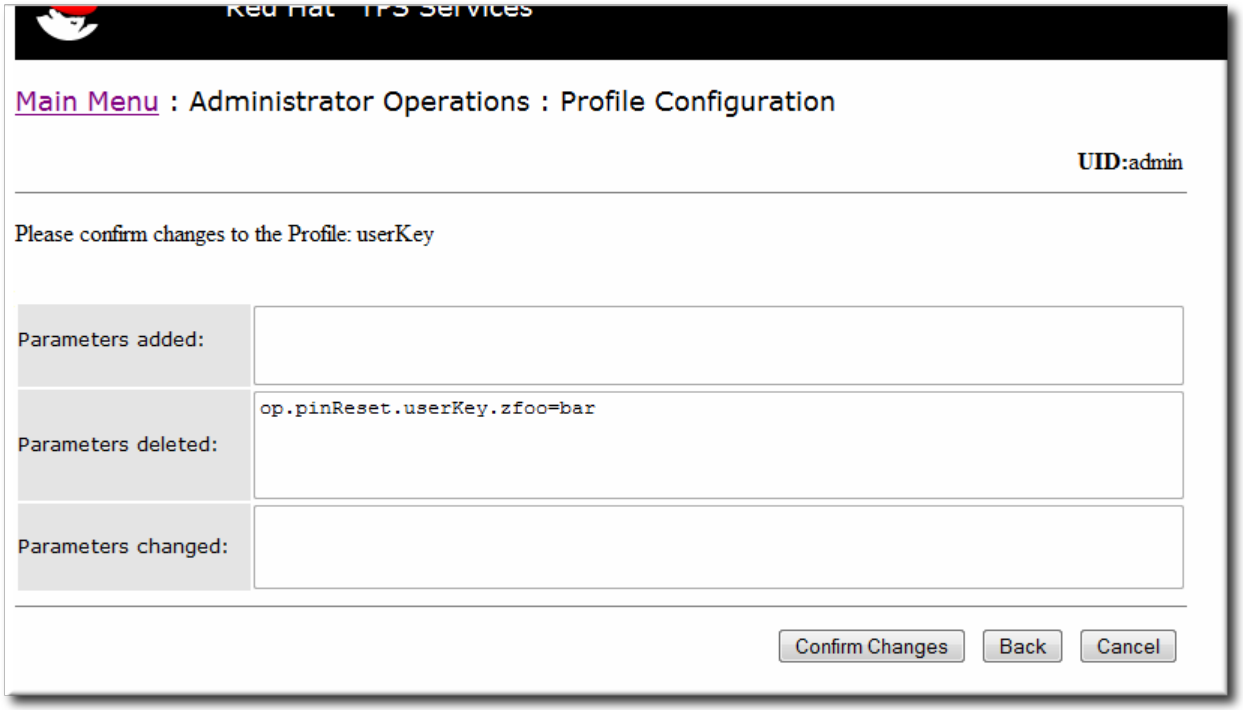
To save a draft of the profile, click the **Save** button, which preserves the current changes. This updates the TPS **CS.cfg**; any other admin users who are editing the TPS configuration will have to edit the updated file, but they can still make changes.



NOTE

An agent can *enable* a profile even if it has not been sent for approval by an administrator.

5. When the profile is submitted, a list of all of the changes comes up, showing both additions and deletions. If the changes are correct, click the **Confirm Changes** button.

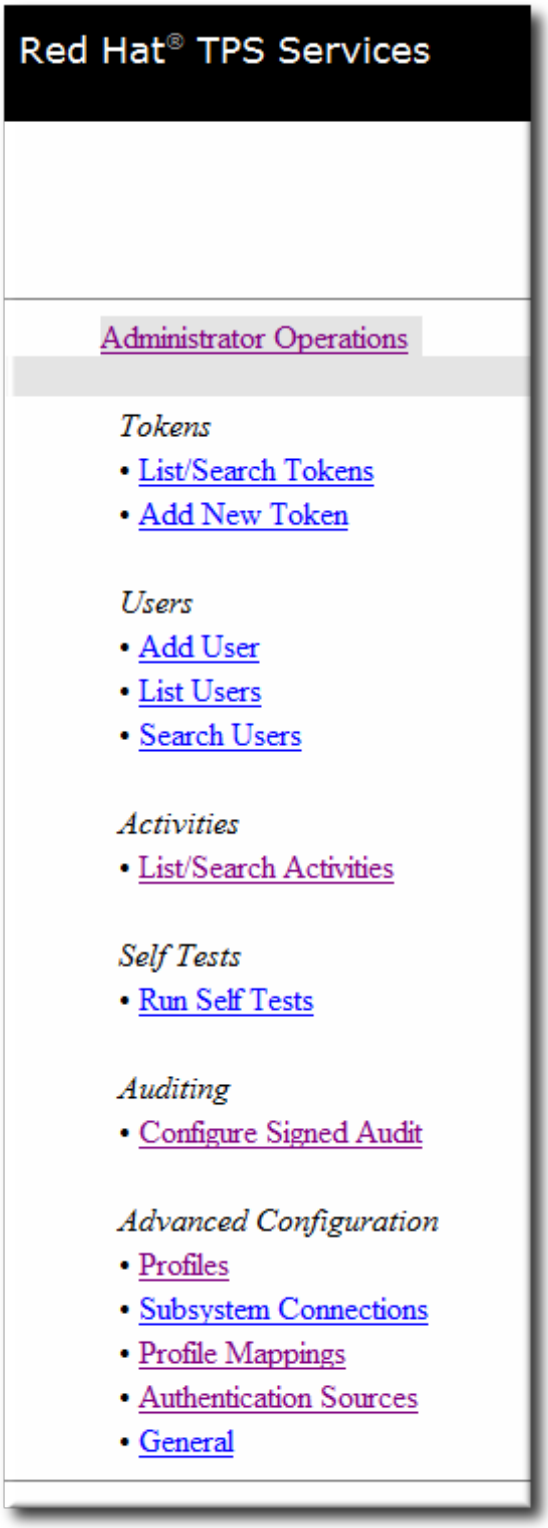


A new profile can be added in the same way: give it a name, paste in the new configuration, validate the settings, and then have it approved by an agent.

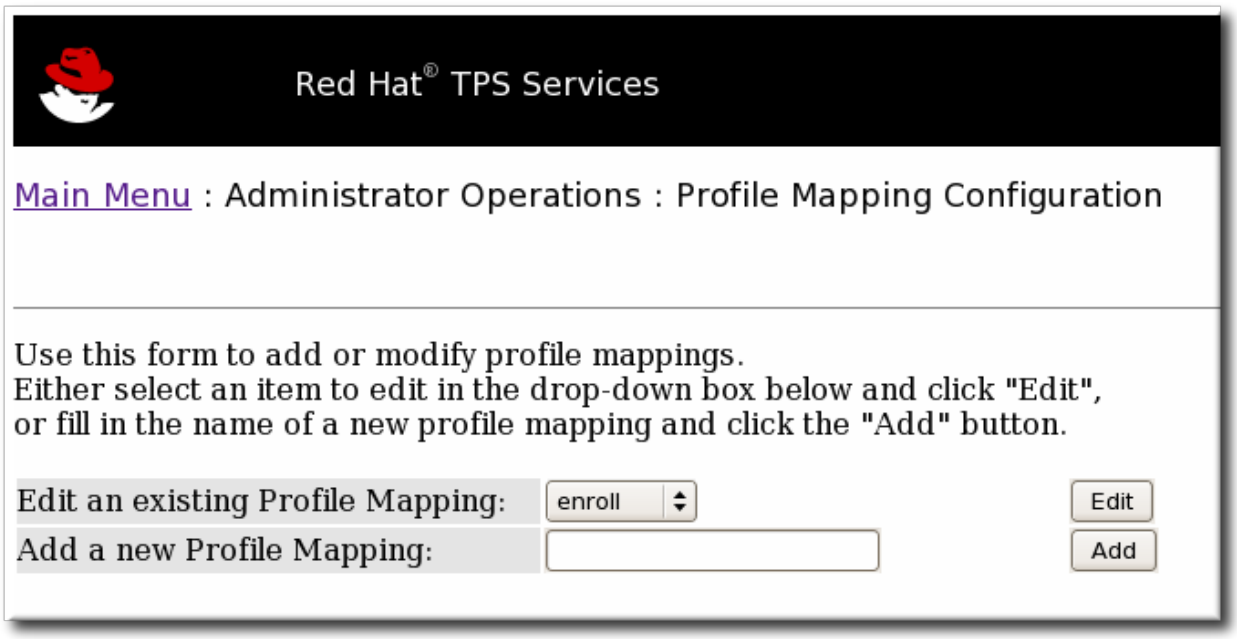
9.4.6.2. Mapping Token Types and TPS Policies

A *mapping* associates a profile with a subset of smart cards which meet certain parameters. This can be used to define policies for specific types of cards and then format them automatically and properly to a certain user based on characteristics in the card.

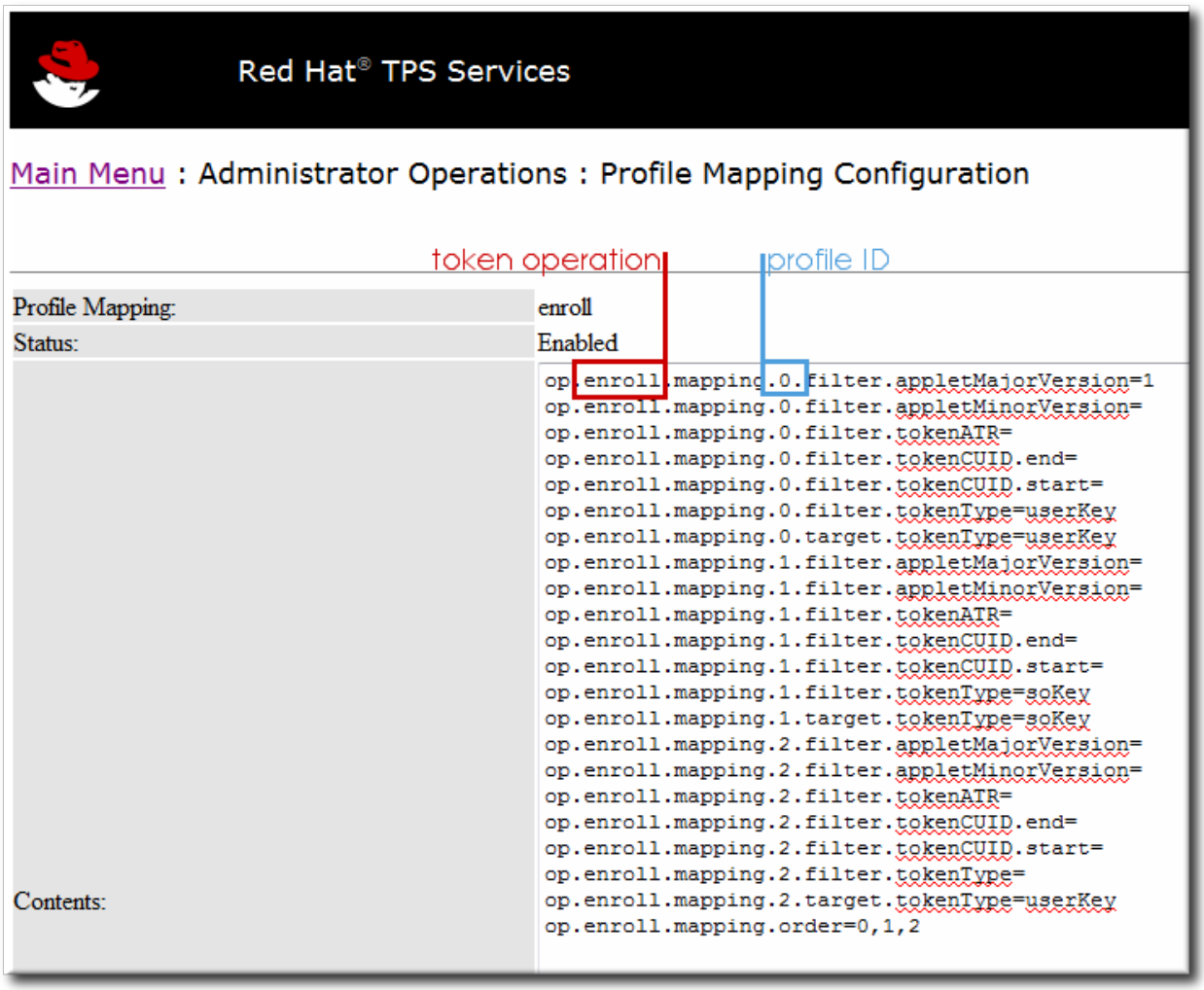
1. In the **Administrator Operations** tab, click the **Profile Mappings** link.



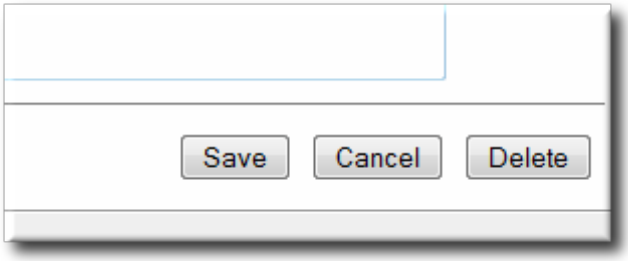
2. Select the profile from the drop-down menu.


Red Hat® TPS Services
Main Menu : Administrator Operations : Profile Mapping Configuration
Use this form to add or modify profile mappings.
Either select an item to edit in the drop-down box below and click "Edit",
or fill in the name of a new profile mapping and click the "Add" button.
Edit an existing Profile Mapping:
enroll
Edit
Add a new Profile Mapping:
Add

3. Edit the mapping parameters.



4. Click **Save**.

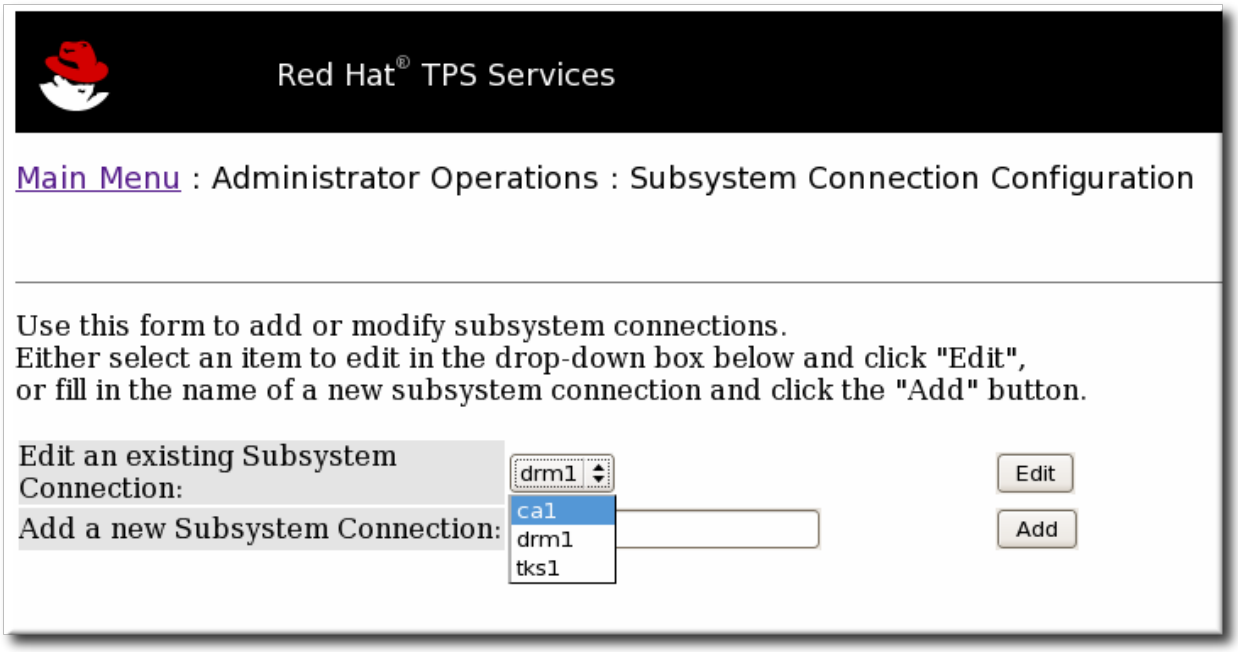


9.4.6.3. Configuring Connections to Other Subsystems

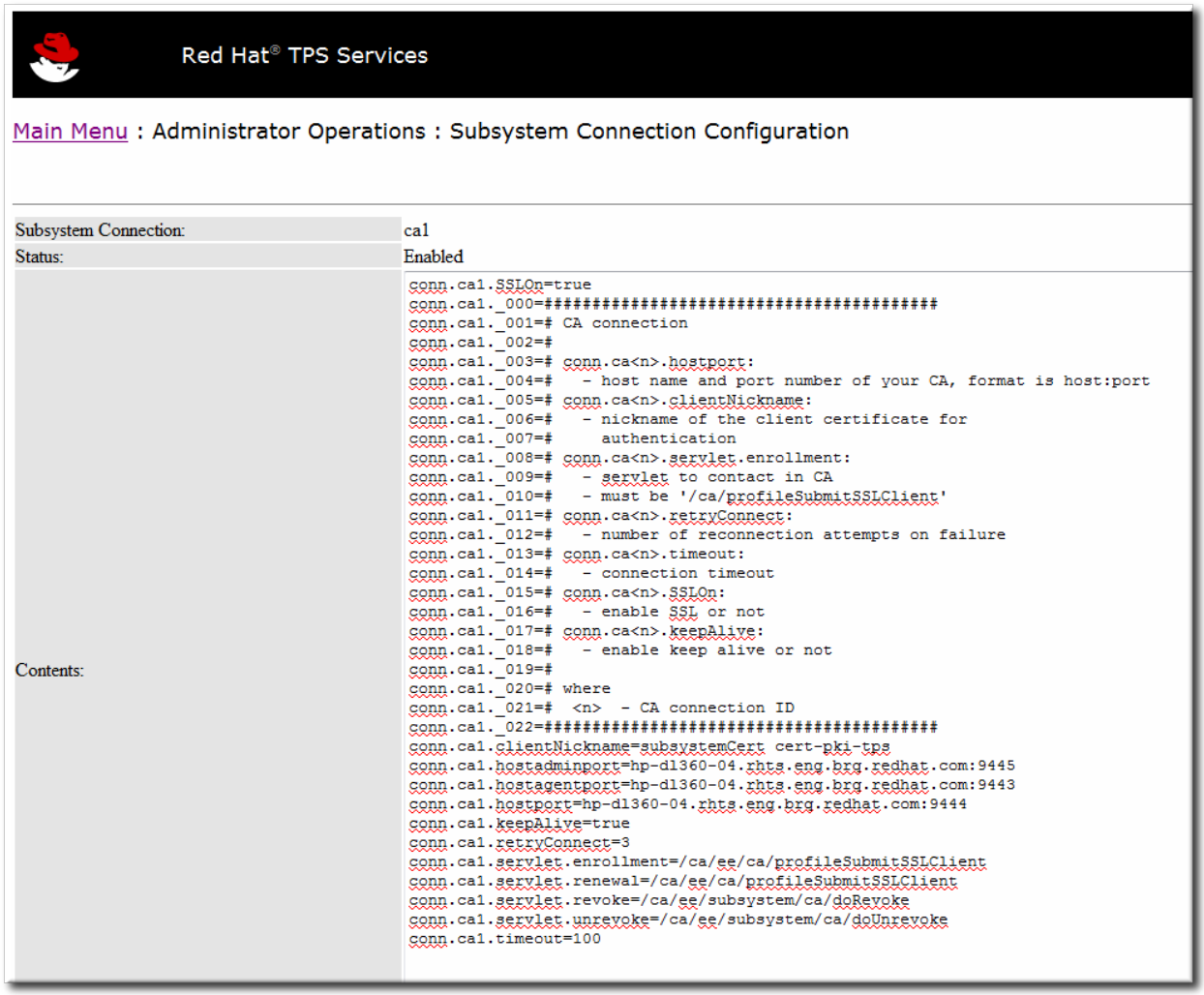
Every TPS has connections configured to at least one CA and one TKS instance, and optionally a DRM instance. These default connections can be edited and additional connections can be added for failover tolerance or for load balancing.

Each connection — meaning each CA, TKS, and DRM that the TPS uses — has a separate entry in the **`CS.cfg`** file.

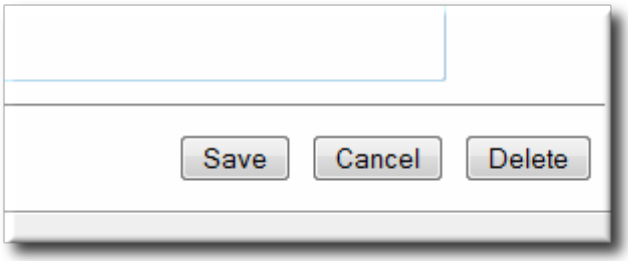
1. In the **`Administrator Operations`** tab, select the **`Subsystem Connections`** link.


Red Hat® TPS Services
Main Menu : Administrator Operations : Subsystem Connection Configuration
Use this form to add or modify subsystem connections.
Either select an item to edit in the drop-down box below and click "Edit",
or fill in the name of a new subsystem connection and click the "Add" button.
Edit an existing Subsystem Connection:
drm1
ca1
drm1
tks1
Edit
Add a new Subsystem Connection:
Add

2. Edit the subsystem connection settings, such as the hostname, servlets, and certificate information.



3. Click **Save**.

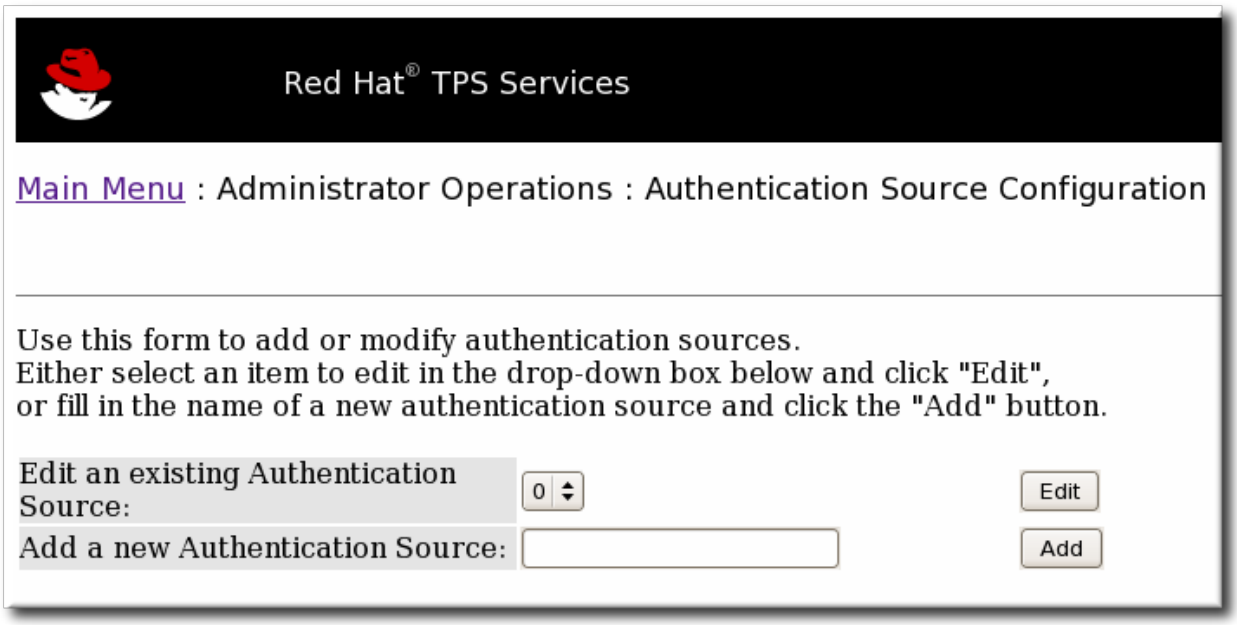


A new subsystem connection can be added in the same way: give it a name, paste in the new configuration, and validate the settings.

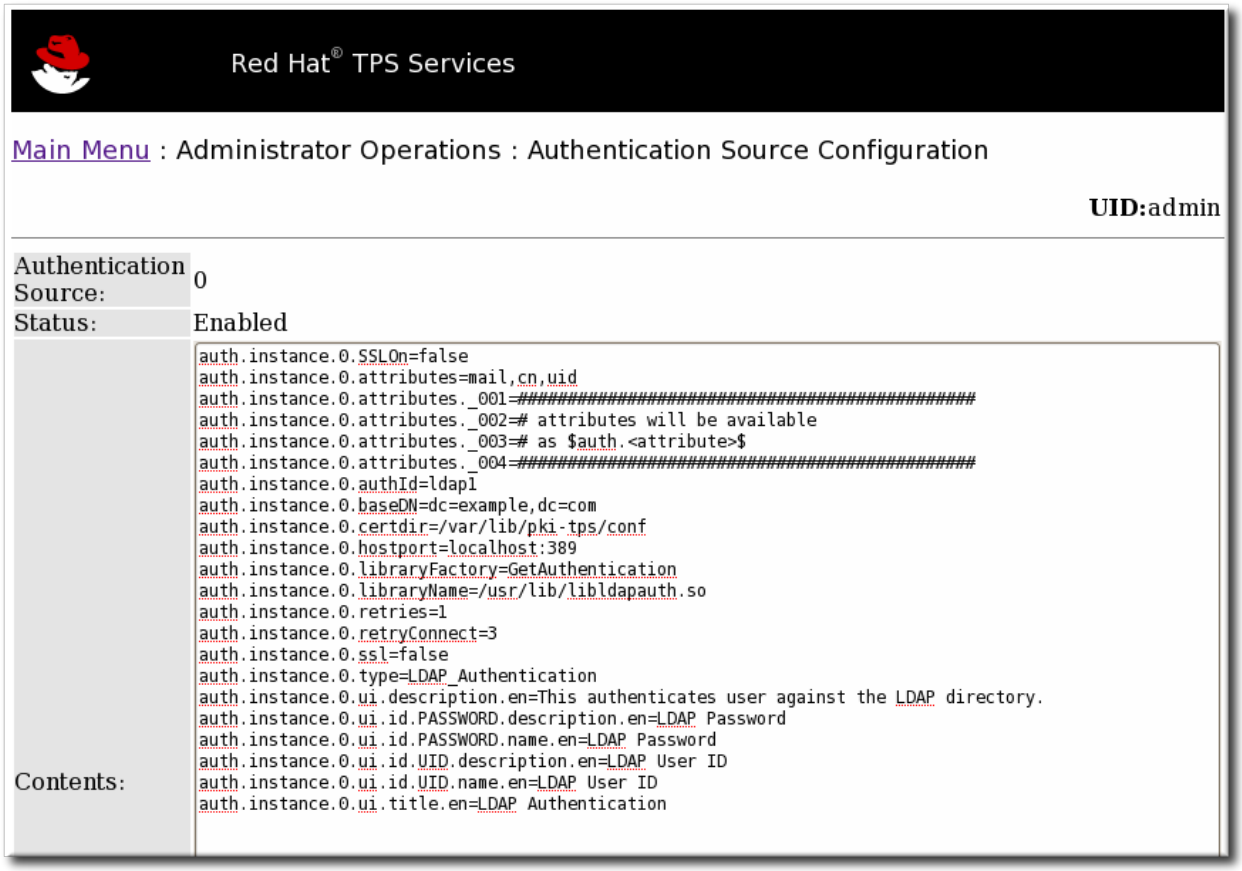
9.4.6.4. Editing LDAP Authentication Sources

The authentication directory is the LDAP directory that the TPS checks for end user credentials to process token operations.

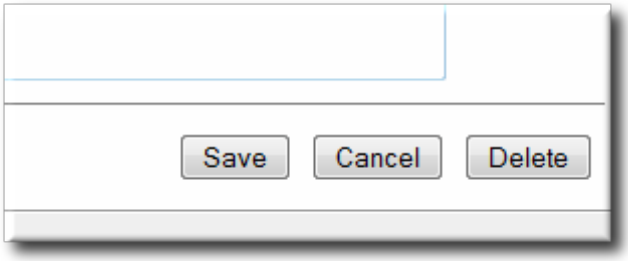
1. In the **Administrator Operations** tab, select the **Authentication Sources** link.
2. Select the authentication instance (identified by the number) from the drop-down menu.


Red Hat® TPS Services
Main Menu : Administrator Operations : Authentication Source Configuration
Use this form to add or modify authentication sources.
Either select an item to edit in the drop-down box below and click "Edit",
or fill in the name of a new authentication source and click the "Add" button.
Edit an existing Authentication Source:
0
Edit
Add a new Authentication Source:
Add

3. Edit the LDAP server connection settings.



4. Click **Save**.



A new LDAP authentication source can be added in the same way: give it a name, paste in the new configuration, and validate the settings.

9.4.6.5. Setting TPS Server General Configuration

There are some general configuration elements for the TPS, which do not fit in with major configuration areas:

- The default and maximum number of entries returned for LDAP searches (the token database, internal database, and authentication directory)
- The maximum search time, in seconds for LDAP searches (the token database, internal database, and authentication directory)
- Minimum password length
- Secure channel settings

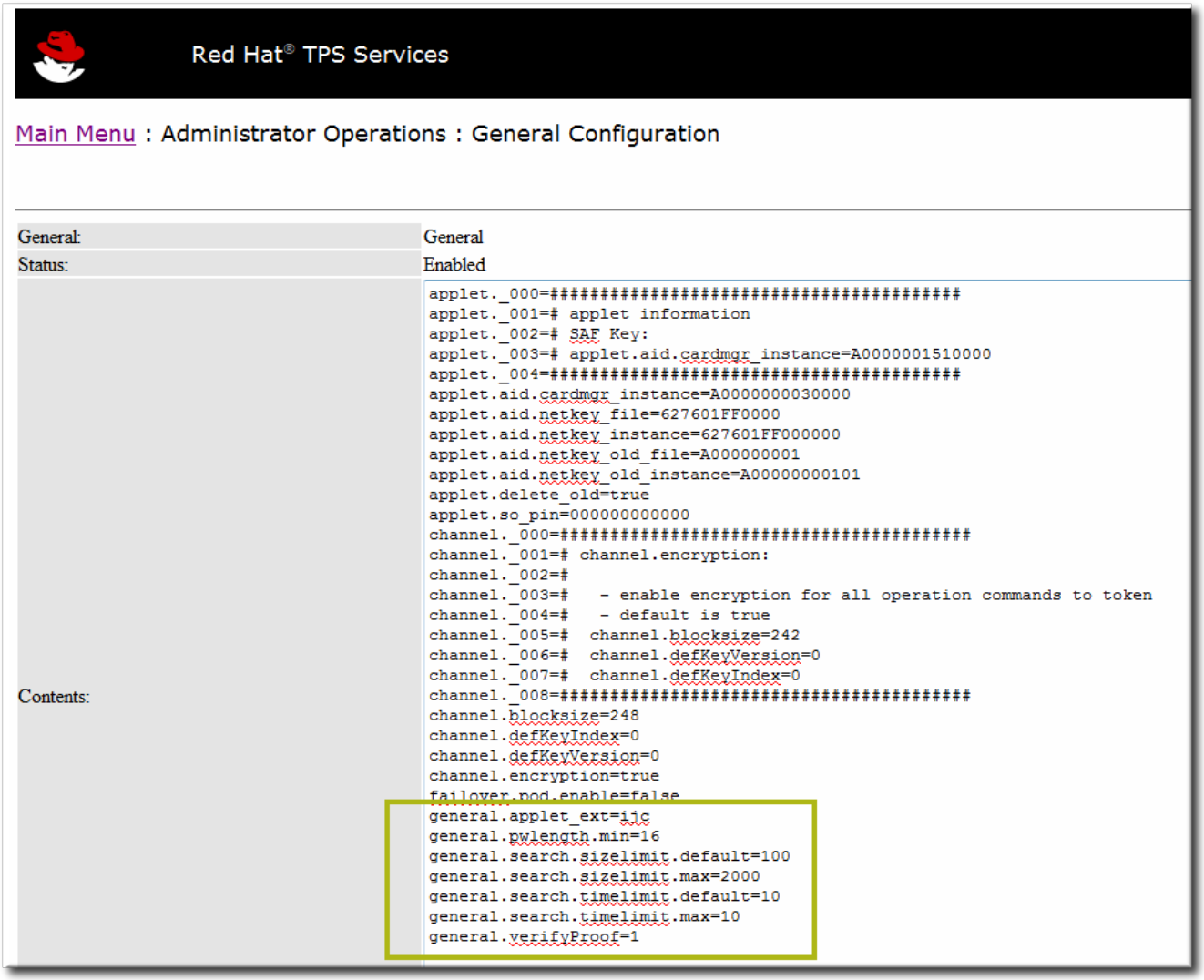


Figure 9.19. General Configuration: Search Setup

The search and password parameters are fairly straightfoward. The search parameters govern searches against any of the LDAP directories used by the TPS for settings, tokens, and users. THe password relates specifically to passwords used by TPS users.

The last general configuration area defines the secure channel characteristics that are used to

configure with the Enterprise Security Client. This channel can be configured for four attributes:

- Its size
- Encryption
- The encryption key version and type

Example 9.1. Default TPS-Token Channel Configuration

```
channel.blocksize=248
channel.defKeyIndex=0
channel.defKeyVersion=0
channel.encryption=true
```

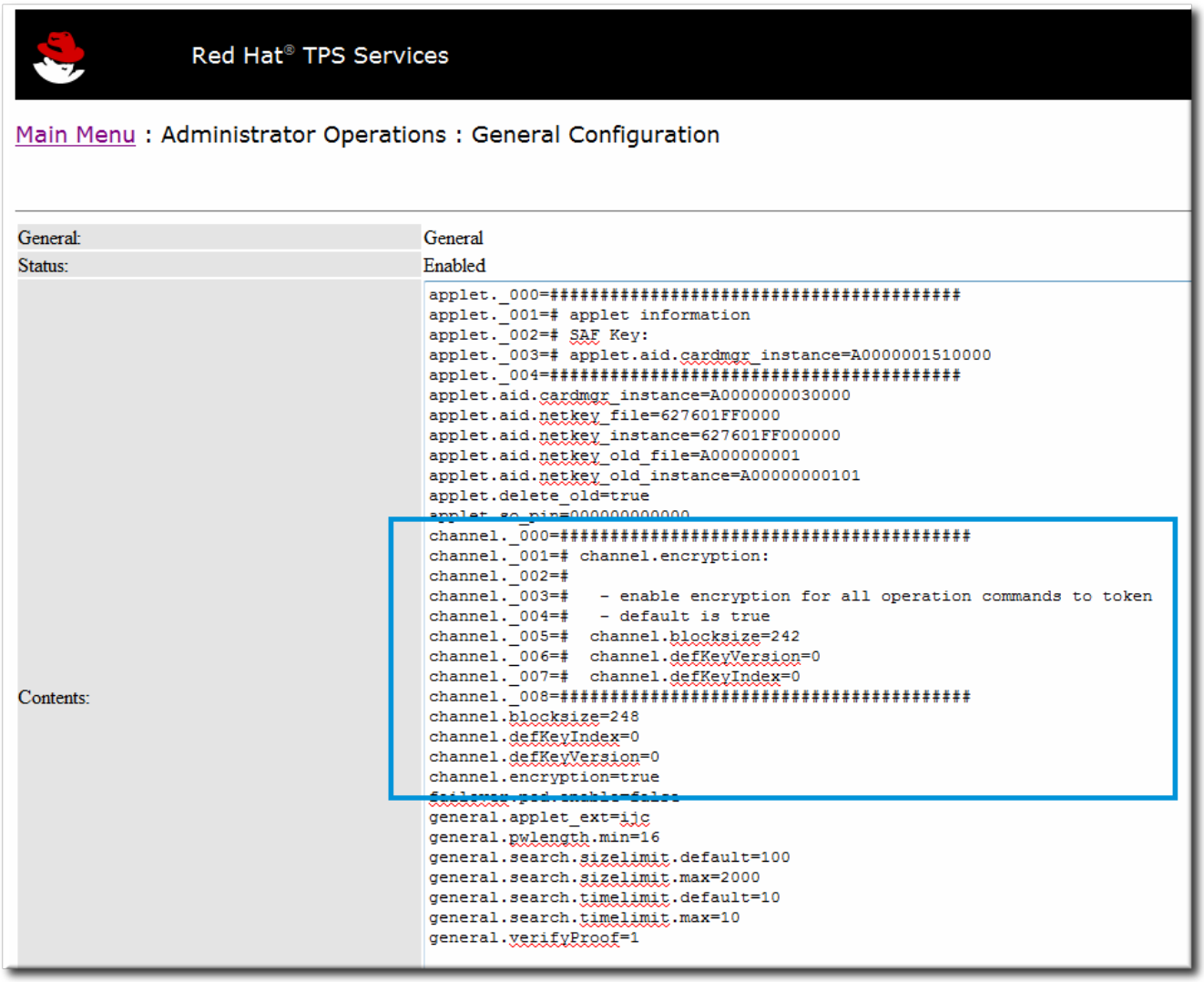


Figure 9.20. General Configuration: Channel Setup

9.5. Conflicting Token Certificate Status Information

The TPS stores the complete history of certificates' status, so that all changes in status can be reviewed. However, the status shown on the token is that last status of the certificate at the time the

token was formatted. The status of the certificates on the token may not immediately reflect the real status of the certificates. It is possible to have multiple tokens with the same certificate information on them; it then is possible for the certificate status on these tokens to become out of sync with the status information in the CA database. When viewing these tokens in the TPS agents page, then, the certificate information can be inconsistent.

For example, Token #1 has two certificates stored on it, an encryption certificate (Encrypt #1) and a signing certificate (Signing #1). If Token #1 is lost, then both of its certificates are revoked, so both Encrypt #1 and Signing #1 are marked as revoked. When the user is issued a new token, Token #2, then Encrypt #1 is recovered, and a new signing certificate, Signing #2, is issued. The status for the three certificates, then, is as follows:

- Signing #1 - revoked
- Signing #2 - active
- Encrypt #1 - active

If Token #1 is found, then the certificates for Token #2 are revoked and the certificates for Token #1 are reactivated. The status for the three certificates, then, is as follows:

- Signing #1 - active
- Signing #2 - revoked
- Encrypt #1 - active

Through the TPS agent's page, however, viewing Token #1 shows Signing #1 is active; viewing Token #2 shows that Signing #1 is revoked. This is because that Signing #1 was still revoked when Token #2 was formatted, and that information was not updated when Token #1 was subsequently formatted.

To find the current status of certificates, view an active token, and list the certificates. Active tokens always have the most current certificate status. For information on listing certificates stored on tokens, see Section 9.3.1, “Searching Tokens”.

Index

A

accessing end-entity gateways , Certificate System Users

accessing forms, Accessing Agent Services

agent services forms

- accessing , Accessing Agent Services
- Certificate Manager , Certificate Manager Agent Services
- Data Recovery Manager , Data Recovery Manager Agent Services
- Online Certificate Status Manager , Online Certificate Status Manager Agent Services
- Registration Manager, Registration Manager Agent Services
- TPS, Token Processing System Agent Services

agents

- requirements for , Agent Tasks
- responsibilities , Agent Tasks

C

CA

- built-in OCSP service , Certificate Manager

certificate authorities (CAs) , Overview of Certificate System

Certificate Manager
- agent services forms , Certificate Manager Agent Services
- built-in OCSP service , Certificate Manager
- overview , Certificate Manager

certificate profile
- approving , Enabling or Disabling a Certificate Profile
- certificate profile information , Viewing Certificate Profile Information
- disabling , Enabling or Disabling a Certificate Profile
- end user certificate profile , Viewing Certificate Profile Information
- policy information , Viewing Certificate Profile Information
- processing requests , Approving Requests

certificate requests
- approving , Approving Requests
- examining , Selecting a Request
- handling process , Managing Requests
- listing , Listing Certificate Requests
- statuses , Listing Certificate Requests
- types of , Listing Certificate Requests

certificate status, Conflicting Token Certificate Status Information

Certificate System
- directory server and , CA: Publishing to a Directory
- overview , Overview of Certificate System
- subsystems , Certificate Manager

certificates
- conflicting status, Conflicting Token Certificate Status Information
- finding , CA: Finding and Revoking Certificates
- issuing to requester , Sending an Issued Certificate to the Requester
- searching for , Searching for Certificates (Advanced), Searching for Certificates (Advanced)
- taking off hold, Taking Ceritificates Off Hold

cloning enrollment requests , Managing Requests

cryptography concepts , Required Concepts

D

Data Recovery Manager , DRM: Recovering Encrypted Data
- agent services forms , Data Recovery Manager Agent Services
- overview , Data Recovery Manager

Directory Server
- Certificate System and , CA: Publishing to a Directory

E

end entities , Overview of Certificate System

enrollment requests
- approving , Approving Requests
- cloning , Managing Requests
- examining , Selecting a Request
- handling process , Managing Requests
- listing , Listing Certificate Requests
- statuses , Listing Certificate Requests

F

forms
- accessing , Accessing Agent Services

I

introduction , Overview of Certificate System

issuing a certificate , Sending an Issued Certificate to the Requester

L

List Requests form , Listing Certificate Requests

M

managers, overview , Certificate Manager

N

notification of issuance , Sending an Issued Certificate to the Requester

O

Online Certificate Status Manager , Online Certificate Status Manager: Verifying Certificate Status
- agent services forms , Online Certificate Status Manager Agent Services
- overview , Online Certificate Status Manager

online certificate validation authority
- defined , Online Certificate Status Manager

P

PKI (public-key infrastructure) , Overview of Certificate System

prerequisites , Required Concepts

privileged operations and users , Agent Tasks

profiles , CA: Working with Certificate Profiles
- about , About Certificate Profiles
- approving and disapproving , Enabling and Disabling Certificate Profiles
- enabling and disabling , Enabling and Disabling Certificate Profiles
- how profiles work , About Certificate Profiles
- working with , CA: Working with Certificate Profiles

R

Registration Manager
- agent services forms , Registration Manager Agent Services
- overview , Registration Manager

Request details form , Selecting a Request

Request Queue form , Listing Certificate Requests

request status, on List Requests form , Listing Certificate Requests

requests
- approving , Approving Requests

requests, enrollment
- cloning , Managing Requests
- examining , Selecting a Request
- handling process , Managing Requests
- listing , Listing Certificate Requests
- statuses , Listing Certificate Requests
- types of , Listing Certificate Requests

revoking certificates
- taking certificate off hold, Taking Ceritificates Off Hold

S

security concepts , Required Concepts

servlet
- XML parameter, Using Java Servlets with Subsystem Web Forms

status of requests , Listing Certificate Requests

subsystems, overview , Certificate Manager

T

Token Processing System, TPS: Managing Token and Smart Card Operations

TPS

- adding users, Adding Users
- agent services forms , Token Processing System Agent Services
- certificates
    - conflicting stat, Conflicting Token Certificate Status Information
- certificates and tokens, TPS: Managing Token and Smart Card Operations
- changing token status, Changing Token Status
- deleting tokens, Deleting the Token
- setting profiles, Setting Profiles for Users
- users, Managing TPS Users